KnowBe4

PHISHING BENCHMARKING 2024 RAPPORT POUR L'EUROPE

INTRODUCTION

Année après année, la cybercriminalité monte en puissance, jetant ses filets de plus en plus loin et piégeant un nombre croissant de victimes tant dans les sphères professionnelles que personnelles. Les cybercriminels n'affichent aucune préférence, et ciblent tous les utilisateurs, partout et à tout moment. Face à des mécanismes de cyberdéfense qui se perfectionnent en permanence, les agresseurs changent de stratégie en tentant d'exploiter une autre cible : l'être humain, plus vulnérable et plus facile à berner. L'humain et sa fragilité restent un vecteur d'attaque toujours intéressant pour les cybercriminels, qui ciblent des victimes individuelles de tous les milieux et de tous les horizons, et occupant des rôles différents au sein des organisations. De nombreuses organisations investissent de façon disproportionnée dans des garde-fous technologiques, mais négligent souvent le rôle crucial de la gestion du risque humain.

À l'heure où l'intelligence artificielle (IA) devient omniprésente dans toutes les dimensions de la technologie, la vigilance en matière de cybersécurité n'a jamais été aussi importante. Les systèmes d'IA peuvent analyser des ensembles de données volumineux et repérer des tendances avec une efficacité et une rapidité qui dépassent largement les facultés humaines. L'IA s'avère ainsi une arme à double tranchant : elle permet en effet de renforcer considérablement les mesures de cybersécurité, mais elle fournit aussi aux pirates des outils sophistiqués qui leur permettent d'exploiter les vulnérabilités.

Les cybercriminels combinent les tactiques bien connues avec des techniques avancées pour faire tomber les défenses des domaines numériques et saper les mesures de sécurité axées sur l'humain. Une protection efficace implique de sensibiliser les employés et de leur faire acquérir des habitudes et des comportements à l'appui d'une culture de la sécurité robuste. Chaque membre d'une organisation doit se percevoir comme faisant partie intégrante du système de défense contre les cyberattaques et être conscient des répercussions de ses actions sur la sécurité globale.

Les cybercriminels exploitent les vulnérabilités humaines. Ils mettent à profit le manque de connaissances, les distractions et les excès de confiance et jouent sur le tableau de l'émotionnel. Ces tactiques axées sur l'humain se sont révélées très efficaces, car même les mesures techniques de sécurité les plus robustes peuvent être fragilisées par l'erreur ou la sensibilisation insuffisante d'un seul employé.

Les responsables de la sécurité doivent anticiper la réaction des employés lorsqu'ils reçoivent des e-mails d'hameçonnage : vont-ils cliquer sur le lien ? Tomber dans le piège et transmettre des identifiants ? Télécharger une pièce jointe contenant un programme malveillant ? Vont-ils simplement ignorer l'e-mail ou le supprimer sans prévenir leur équipe de sécurité ? Ou bien vont-ils signaler une suspicion d'attaque par hameçonnage et jouer un rôle actif dans la ligne de défense humaine ? En fournissant à leurs employés les connaissances, les compétences et les outils dont ils ont besoin pour identifier les menaces potentielles et y répondre, les organisations peuvent les aider à ne plus être des proies et au contraire à se muer en défenseurs efficaces.

ANALYSE DU RISQUE PAR SECTEUR

La métrique qui représente la vulnérabilité d'une organisation aux tentatives d'hameçonnage est appelée le Pourcentage de Phish-Prone (PPP). En exprimant leur vulnérabilité à l'hameçonnage en termes quantifiables, les dirigeants d'entreprise ont les moyens d'évaluer leur exposition au risque de violation de sécurité et de mettre en place une formation ciblée pour mieux armer leurs collaborateurs contre les cybermenaces.

Le PPP d'une organisation indique le pourcentage de ses employés qui sont susceptibles de tomber à tout moment dans le piège d'une attaque par ingénierie sociale ou par hameçonnage. Il s'agit donc d'un bon indicateur du niveau de risque d'une organisation et de sa résilience face à ces attaques.

Plus le PPP est élevé, plus le risque est grand, car il signifie qu'un plus grand nombre d'employés aura tendance à se laisser piéger. Inversement, un PPP peu élevé signifie que la ligne de défense humaine d'une organisation renforce sa sécurité plus qu'elle ne la met en péril. Un faible PPP est donc optimal, puisque cela démontre que le personnel possède les bons réflexes en matière de sécurité et sait reconnaître et désamorcer ces tentatives.

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 pour l'ensemble des secteurs, par taille d'organisation et par régions géographiques. Ce guide offre une vue d'ensemble des principales conclusions pour l'Europe.

RAPPORT « GLOBAL PHISHING BY INDUSTRY BENCHMARKING STUDY » 2024

Toute organisation aspire à évaluer ses performances par rapport à ses homologues dans son secteur d'activité, mais pour que la comparaison soit significative, il est nécessaire de disposer de données complètes et d'avoir recours à une méthode validée scientifiquement pour obtenir des résultats crédibles. Beaucoup d'organisations ont bien du mal à estimer leur positionnement par rapport à leurs homologues.

C'est là que notre rapport comparatif annuel sur l'hameçonnage par secteur entre en jeu. Pour leur apporter une réponse nuancée et précise, le rapport de 2024 a analysé un jeu de données couvrant plus de 54 millions de simulations de tests d'hameçonnage auprès de 11,9 millions d'utilisateurs dans 55 675 organisations 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. Le PPP de chaque organisation a été calculé en mesurant le pourcentage d'employés qui ont cliqué sur une simulation de lien d'hameçonnage ou ouvert une simulation de pièce jointe contenant un programme malveillant au cours d'une campagne de test de KnowBe4.

Dans notre rapport 2024, nous poursuivons notre étude des phases de référence suivantes :

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

VALEURS DE RÉFÉRENCE SUR L'HAMEÇONNAGE AU NIVEAU INTERNATIONAL EN 2024

Phase une

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

Phase deux

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

Phase trois

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

		RÉFÉRENCE			90 JOURS			1 AN		
	Taille de l'organisation (effectif)	De 1 à 249	De 250 à 999	> 1 000	De 1 à 249	De 250 à 999	> 1 000	De 1 à 249	De 250 à 999	> 1 000
RÉGION	Amérique du Nord	29 %	32,6 %	39,1 %	19,8 %	19,9 %	17,9 %	4,3 %	4,6 %	4,6 %
			TOTAL : 35,1 %			**TOTAL : 18,9 %**			**TOTAL : 4,5 %**	
	Afrique	29,7 %	32,8 %	38 %	23,7 %	28,7 %	20,2 %	3,6 %	5,4 %	6,2 %
			TOTAL : 36,7 %			**TOTAL : 22 %**			**TOTAL : 5,9 %**	
	Asie	31,5 %	31,6 %	27,4 %	20,3 %	17,6 %	16,6 %	5,4 %	4,5 %	5,9 %
			TOTAL : 28,4 %			**TOTAL : 17 %**			**TOTAL : 5,5 %**	
	Australie et Nouvelle-Zélande	27,8 %	32,5 %	40,3 %	21,4 %	20,3 %	16,5 %	4,9 %	5,3 %	4,7 %
			TOTAL : 34,4 %			**TOTAL : 19,1 %**			**TOTAL : 5 %**	
	Europe	26,5 %	26,9 %	35,6 %	19,3 %	20,2 %	20,6 %	4,1 %	4,9 %	5,9 %
			TOTAL : 32,6 %			**TOTAL : 20,3 %**			**TOTAL : 5,5 %**	
	Amérique du Sud	32,7 %	29,4 %	44,9 %	24,4 %	22,5 %	16,8 %	5,2 %	5,2 %	3 %
			TOTAL : 39,2 %			**TOTAL : 18,7 %**			**TOTAL : 3,9 %**	
	Royaume-Uni et Irlande	26,5 %	30,2 %	35,2 %	20 %	21 %	16,5 %	4,1 %	4,3 %	4,8 %
			TOTAL : 32,3 %			**TOTAL : 18,4 %**			**TOTAL : 4,5 %**	

EUROPE

Par Martin Kraemer

Données de référence

Le rapport de 2024 fait état d'un déclin des performances des organisations par rapport aux résultats du rapport de 2023. Toutes tailles d'organisation confondues, les performances de référence ont baissé de 3,2 %, les performances sur 90 jours ont augmenté de 0,6 % et les performances sur un an ont baissé de 1,5 %. Les organisations européennes des trois différentes catégories de taille (effectif de 1 à 249, de 250 à 999 et de plus de 1 000 employés) enregistrent des performances supérieures à la moyenne mondiale. Ce sont les petites organisations (26,5 %) qui affichent les meilleures performances avant formation, suivies par les organisations de taille moyenne (26,8 %) et les grandes organisations (35,6 %). Ces chiffres n'ont quasiment pas changé par rapport à l'année dernière et correspondent plus ou moins à ceux des années précédentes. Cette stagnation des résultats laisse à penser que de nombreuses organisations ont besoin de renforcer leurs initiatives de sensibilisation à la sécurité. Elles doivent prendre conscience que le facteur humain est une composante cruciale de leur cyberdéfense et que l'hameçonnage reste le vecteur d'attaque numéro un de l'ingénierie sociale. Il y a toutefois matière à espérer, car les organisations européennes affichent en moyenne de meilleures performances avant formation que leurs homologues dans le reste du monde.

Profil d'organisation type

L'Europe compte un nombre croissant de petites et moyennes entreprises. La vaste majorité des entreprises emploie entre 10 et 49 personnes et moins de 1 % des organisations comptent plus de 250 employés. Plus de 70 % des petites organisations ont une intensité numérique faible ou très faible, selon un rapport d'Eurostat. Les organisations de taille moyenne dont la transformation numérique est à un stade plus avancé (environ 40 % seulement ont un classement faible ou très faible) et moins de 20 % des grandes organisations entrent dans cette catégorie. Cet indicateur se fonde sur plusieurs métriques, telles que l'utilisation d'outils de travail à distance et de logiciels de conférence en ligne, l'existence de mesures de sécurité et l'utilisation de robots dans le secteur manufacturier.

Les petites et moyennes entreprises sont fréquemment la cible de cyberattaques, qu'il s'agisse d'administrations locales, de sous-traitants ou de fournisseurs. Ces organisations sont désormais régulièrement attaquées et doivent donc se préparer. La compromission des e-mails des fournisseurs devient courante, car les fournisseurs servent de passerelles d'accès à leurs partenaires commerciaux. Ces grandes organisations sont en effet les cibles les plus lucratives des cybercriminels.

Problèmes les plus fréquents

Selon le rapport de l'Agence européenne pour la cybersécurité sur le paysage des menaces ENISA Threat Landscape 2023, les organisations en Europe sont fréquemment la cible d'attaques par déni de service distribué et par rançongiciels. Mais si les attaques d'ingénierie sociale utilisant l'IA et d'autres nouvelles techniques sont en hausse, l'hameçonnage demeure le vecteur d'attaque numéro un. L'Europe n'a en outre pas échappé aux nouvelles tactiques d'extorsion qui ont cours dans le monde entier du fait de la professionnalisation continue par les cybercriminels de leurs programmes en tant que service. Le secteur le plus attaqué a été celui des administrations publiques, suivi des particuliers et du secteur de la santé. L'Agence européenne pour la cybersécurité (ENISA) signale également une hausse de la manipulation de l'information dans le contexte de la guerre de la Russie en Ukraine et plus généralement, une accentuation des motivations géopolitiques des cybercriminels.

Dans l'ensemble, la situation est similaire à celles des années précédentes. Les rançongiciels demeurent l'une des cybermenaces majeures, l'hameçonnage s'imposant comme son vecteur d'attaque le plus courant. La multiplication des attaques visant les chaînes d'approvisionnement mérite aussi d'être surveillée de près.

Impact économique

Le véritable impact du cybercrime est difficile à déterminer, mais les cas individuels prouvent la gravité des conséquences des violations de données. Le cumul des conséquences financières a été estimé à environ 0,84 % du produit intérieur brut annuel de l'Europe, selon un rapport d'Upguard de 2018. Depuis, les rançongiciels ont connu de façon répétée une croissance à deux chiffres, année après année. Il est peu probable que le cybercrime ralentisse prochainement, d'autant qu'il est désormais **considéré comme la troisième plus grande économie du monde**.

Les répercussions économiques en Europe peuvent également être évaluées au vu de la gravité des violations de données récentes. On peut citer le cas, en France, du piratage de deux opérateurs gérant le tiers payant pour le compte de mutuelles et d'assurances santé, se soldant par le vol des données de 33 millions de citoyens français, ou encore les conséquences de la faille de sécurité dans le logiciel MOVEit qui ont touché plus de 100 organisations dans toute l'Europe. De nombreuses entités publiques allemandes en font partie. Au Royaume-Uni, les agences de notation avaient conseillé aux clients de geler leurs cotes de crédit. Les gangs de cybercriminels par rançongiciels ont continué leurs violents assauts contre l'Europe, recourant à de nouveaux modes d'extorsion. Les efforts conjoints des autorités chargées de l'application de la loi, coordonnées par Europol, pour faire chuter le gang du rançongiciel LockBit, ont eu pour effet de dévoiler publiquement d'autres violations. Alors que les effets à long terme du démantèlement restent incertains, car les cybercriminels impliqués ont tendance à se regrouper, la perte d'accès à une infrastructure représente un grave revers.

L'Union européenne impose en outre l'un des cadres réglementaires les plus stricts du monde. Le Règlement général sur la protection des données (RGPD), la Directive NIS2 (Network and Information Security) sur la sécurité des réseaux et de l'information et la loi sur la résilience opérationnelle numérique du secteur financier (DORA), entre autres, exigent des organisations qu'elles consacrent des ressources spécifiques. La conformité aux exigences de la législation est obligatoire et son non-respect entraîne de lourdes amendes qui peuvent fortement affecter les résultats des entreprises.

Adoption culturelle et comportement général

Les attitudes vis-à-vis de la sécurité varient beaucoup en Europe. Les facteurs qui entrent en jeu sont la perception de l'importance de la cybersécurité, au même titre que la responsabilité dans un environnement d'entreprise et les moyens dont chacun estime disposer pour se protéger. De façon générale, l'Europe continentale centrale, le Royaume-Uni et l'Irlande sont davantage sensibilisés aux cybermenaces et leurs entreprises sont plus matures en matière de cybersécurité. Cette constatation est corroborée par les conclusions du **Rapport sur la culture de la sécurité** de KnowBe4, qui révèle que la compréhension de la cybersécurité et la hiérarchisation de ses priorités en entreprise sont moins avancées en Europe de l'ouest, de l'est et du sud par rapport à d'autres régions du Vieux continent.

En ce qui concerne la sensibilisation à la sécurité, il est de plus en plus admis que la totalité du personnel doit faire partie de la cyberdéfense d'une organisation. Les organisations de toutes tailles et de tous secteurs confondus ont compris l'importance de responsabiliser leurs collaborateurs pour qu'ils contribuent à la protection de l'entreprise. Toutefois, la capacité de cette prise de conscience à impulser un changement stratégique qui imposerait la cybersécurité comme une priorité de l'entreprise varie sensiblement. Même si la cybersécurité n'est plus considérée comme un simple exercice de routine et est devenue une initiative stratégique, la mise en œuvre des changements indispensables progresse avec lenteur.

Seulement 32 à 35 % des organisations européennes évaluent leurs cyberrisques plus d'une fois par an, selon le rapport sur l'état de la sécurité **ISACA State of Cybersecurity Report 2023**. Ce chiffre, qui a peu varié au cours des trois dernières années, met en évidence les difficultés rencontrées par les organisations à mettre en adéquation les ressources avec les exigences. Elles se heurtent notamment à de constantes restrictions budgétaires et à la pénurie de compétences en cybersécurité, qui reste l'un des défis majeurs. Il n'y a en effet tout simplement pas assez de professionnels disponibles pour pouvoir permettre des avancées importantes.

Influences de l'IA

L'ENISA considère la mésinformation et la désinformation comme des cybermenaces pour les organisations. Le principal exemple est celui des attaques contre les organisations qui soutiennent l'Ukraine contre la Russie. Suite à des campagnes de désinformation, des groupes de cybercriminels ciblent ces organisations. La mésinformation et la désinformation sont désormais alimentées par l'IA, qui permet aux acteurs des menaces de diffuser plus rapidement et plus facilement de fausses informations.

Les organisations en Europe, comme partout ailleurs, ont hâte de tirer les bénéfices d'une adoption précoce des outils optimisés par l'IA générative. Caractérisées par une mentalité traditionnellement plus sensibilisée au risque, de nombreuses entreprises doivent aussi gérer tout un éventail d'enjeux en matière de confidentialité, de sécurité et d'autres questions éthiques, qui les poussent à adopter une approche relativement plus réservée. C'est par exemple ce qui a incité l'organisme de protection de données en Italie à interdire temporairement l'utilisation de ChatGPT. Depuis, l'outil est de nouveau autorisé. Les organisations doivent continuer à former leurs employés et à mettre en place les garde-fous nécessaires pour encadrer l'utilisation d'outils alimentés par l'IA.

Les e-mails d'hameçonnage, en partie alimentés par l'IA, qui inondent le monde entier, touchent aussi les organisations européennes. Ces e-mails conservent les schémas habituels, mais la présence de l'IA est bien visible dans les attaques par harponnage et par faux-semblants. Même si l'hameçonnage optimisé par l'IA en est encore à ses balbutiements, les organisations doivent s'attendre à voir l'hameçonnage en tant que service se professionnaliser et s'automatiser. L'hameçonnage est appelé à rester le principal vecteur d'attaque.

Points à retenir

- ✓ Les organisations européennes enregistrent en moyenne des performances supérieures à celles du reste du monde, signe d'une compréhension croissante de la cybersécurité et d'une sensibilisation générale aux escroqueries en ligne. Ce constat peut en partie être attribué à la rigueur bien connue du paysage réglementaire et juridique en Europe.
- ✓ Les organisations restent un peu à la traîne lorsqu'il s'agit d'engagement sur le long terme. Le PPP des moyennes et grandes entreprises est ainsi inférieur à la moyenne mondiale.
- ✓ L'Europe doit continuer de faire évoluer son système de réglementation en matière de protection des données et d'IA pour rester à l'avant-garde de la cybersécurité, à l'heure où les organisations commencent à adopter des outils d'IA.

EUROPE	RÉFÉRENCE	90 JOURS	1 AN
De 1 à 249	26,5 %	19,3 %	4,1 %
De 250 à 999	26,9 %	20,2 %	4,9 %
> 1 000	35,6 %	20,6 %	5,9 %
PPP moyen toutes tailles d'organisation confondues	32,6 %	20,3 %	5,5 %

Lire le rapport complet