FORTRA

Rapport comparatif 2025 sur les simulations d’hameçonnage

Résultats de l’analyse comparative

Juin 2026

Avant-propos

Il y a quinze ans, l'hameçonnage était relativement simple. Les attaquants copiaient des pages de connexion légitimes, les hébergeaient sur des sites Web compromis ou des domaines similaires, puis diffusaient massivement des courriels usurpés afin de récolter des noms d'utilisateur et des mots de passe. En réponse, de grandes banques, des fournisseurs de services de paiement et des entreprises de messagerie Web ont mis au point DMARC, une norme conçue pour empêcher l'usurpation exacte d'un domaine dans les courriels lorsqu'elle est correctement mise en œuvre.

Les attaquants se sont rapidement adaptés. Plutôt que d'usurper directement des domaines légitimes, ils ont commencé à utiliser des comptes de messagerie gratuits et de nouveaux domaines similaires, misant sur les noms d'affichage et les adresses visuellement semblables pour tromper les utilisateurs.

Les navigateurs ont introduit des avertissements en temps réel pour les sites d'hameçonnage connus, mais ces protections étaient, par nature, réactives. Les premières victimes d'une nouvelle campagne d'hameçonnage demeuraient peu protégées avant que le site soit repéré et ajouté à une liste de blocage. Les fournisseurs de solutions de sécurité du courriel ont réagi en réécrivant les URL et en les analysant au moment du clic, tandis que les entreprises déployaient des passerelles Web sécurisées pour mieux protéger leurs utilisateurs.

Les responsables d'activités d'hameçonnage se sont adaptés de nouveau. Les campagnes d'hameçonnage par code QR se sont révélées particulièrement efficaces, puisqu'elles éloignaient les victimes des appareils d'entreprise renforcés et les dirigeaient vers leurs téléphones intelligents personnels, où les mesures de sécurité organisationnelles étaient souvent absentes ou nettement moins robustes.

L'adoption généralisée de l'authentification multifacteur (AMF) devait réduire considérablement le risque d'hameçonnage. Les attaquants ont plutôt fait évoluer leurs techniques une fois de plus.

Certains groupes se sont tournés vers l'échange frauduleux de carte SIM, en convainquant des fournisseurs de services mobiles de transférer le numéro de téléphone d'une victime vers un appareil contrôlé par l'attaquant. Une fois les identifiants volés, les codes SMS interceptés permettaient de franchir la dernière étape nécessaire pour accéder aux comptes.

D'autres ont eu recours à l'ingénierie sociale. Dans un scénario courant, les attaquants obtenaient d'abord le nom d'utilisateur et le mot de passe d'une victime, puis déclenchaient une demande d'AMF sur le service légitime. La victime recevait ensuite un appel automatisé prétendument de sa banque, l'avertissant d'une activité suspecte. L'appelant lui demandait alors de saisir le code de vérification qu'elle venait de recevoir; sans le savoir, la victime transmettait ainsi le jeton d'AMF à l'attaquant en temps réel.

Des méthodes plus sophistiquées sur le plan technique ont rapidement suivi. Des outils d'hameçonnage de type « attaquant au milieu », ont commencé à relayer des sessions de connexion complètes, transmettant directement aux services légitimes les frappes au clavier, les données de session et les demandes d'authentification. Ces attaques se sont révélées particulièrement efficaces dans les environnements d'entreprise dotés de portails de connexion personnalisés, puisque les victimes voyaient exactement le processus d'authentification attendu. D'autres groupes ont plutôt ciblé le détournement de session, le vol de jetons et la compromission des appareils, contournant entièrement le vol traditionnel d'identifiants.

L'évolution la plus importante est toutefois peut-être l'essor du service d'hameçonnage (Phishing-as-a-Service ou PhaaS). Ces plateformes offrent des modèles d'hameçonnage prêts à l'emploi, une infrastructure de diffusion résiliente et des trousses d'hameçonnage modernes capables de contourner l'AMF au moyen de diverses techniques éprouvées. Ainsi, les opérations d'hameçonnage sophistiquées n'exigent plus de connaissances techniques poussées. Bon nombre d'entre elles peuvent maintenant être lancées à faible coût, avec peu de compétences et en quelques clics seulement.

L'écosystème moderne de l'hameçonnage n'est plus défini par des escroqueries isolées, mais par des plateformes criminelles en évolution rapide qui s'adaptent continuellement aux améliorations défensives. Les tendances étudiées dans le présent rapport montrent comment l'hameçonnage est devenu une industrie évolutive axée sur les services. Compte tenu de cette maturité, il est impératif de miser sur la sensibilisation du facteur humain. La réduction du risque humain par la sensibilisation est essentielle à la protection des écosystèmes organisationnels.

John Wilson
Chercheur principal sur les menaces, Fortra

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

Rapport comparatif 2025 sur les simulations d’hameçonnage

Statistiques comparatives et tendances des taux de réponse

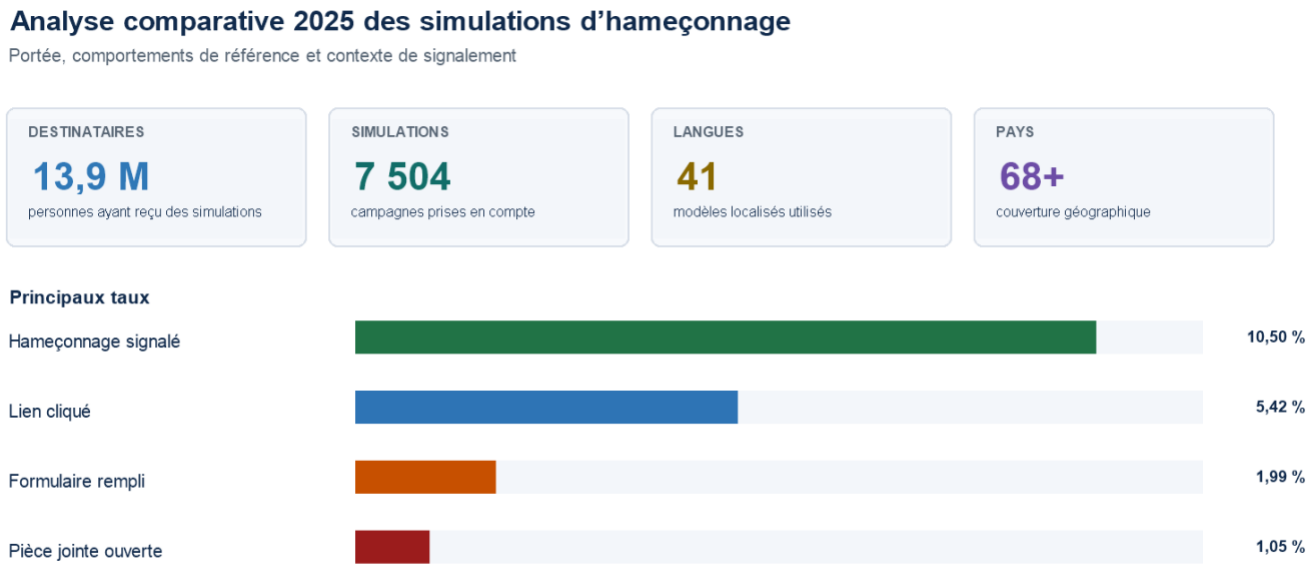

Figure 1. Portée globale de l’analyse comparative et principaux taux de réponse.

Ces chiffres établissent le contexte du reste du rapport : 14 millions de destinataires de simulations répartis dans plus de 7 500 campagnes. À cette échelle, nous pouvons clairement établir la portée des indicateurs présentés dans la suite du rapport.

Comprendre les données comparatives

Un taux de signalement de 10,5 % n’a rien de réjouissant. Cela signifie que 9 tentatives d’hameçonnage sur 10 ne sont pas signalées. Il ne faut pas sous-estimer la valeur du signalement des courriels d’hameçonnage pour les équipes de sécurité internes. Un seul signalement peut déterminer si une campagne d’hameçonnage réussira ou non. Cette statistique, à elle seule, devrait suffire à démontrer qu’une sensibilisation accrue est nécessaire. Le présent rapport indique les régions, les langues, les tailles d’organisation et les secteurs où cette sensibilisation est la plus nécessaire.

Il est facile de croire qu’un taux de clic de 5,42 % ou qu’un taux de soumission de mot de passe de 1,99 % est acceptable parce qu’il est faible. La conversion de ces pourcentages apparemment modestes en nombres absolus révèle l’ampleur de la menace. Plus de 750 000 personnes ont cliqué sur des simulations d’hameçonnage et plus de 250 000 ont fourni leur mot de passe.

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

1. Tendances géographiques du risque

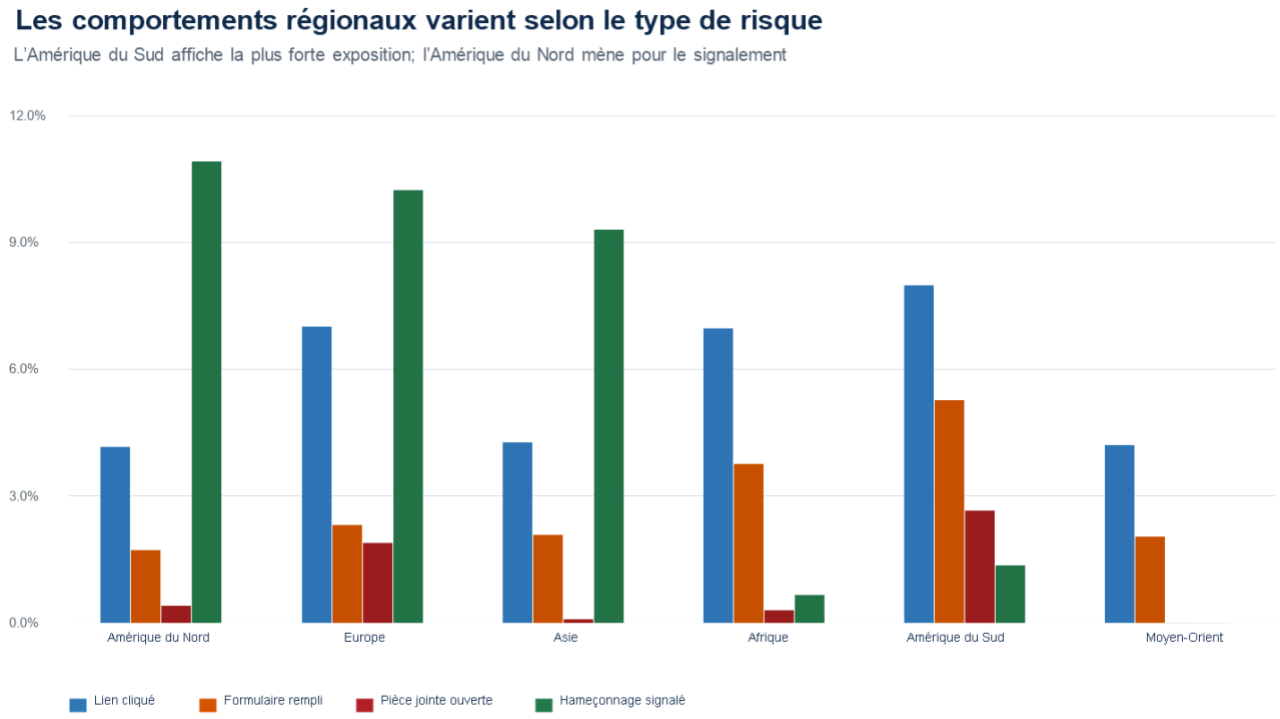

Figure 2. Comparaison régionale des taux de clic, de soumission de formulaire, d'ouverture de pièce jointe et de signalement. Voir l'annexe I, tableau 1.

Les données régionales fournissent un éclairage intéressant sur le comportement des utilisateurs de différentes régions lors des simulations d'hameçonnage.

Une distinction importante se dégage entre l'Amérique du Nord, l'Europe et l'Asie, d'une part, et l'Afrique, l'Amérique du Sud et le Moyen-Orient, d'autre part. Les taux de signalement sont particulièrement faibles dans ces trois dernières régions; le Moyen-Orient affiche le plus faible taux de signalement d'hameçonnage des six régions. Il présente toutefois le plus faible taux de fuite d'identifiants, c'est-à-dire de soumission de formulaire. L'Amérique du Nord obtient le meilleur taux de signalement, suivie de près par l'Europe et l'Asie. En Europe, les taux de soumission de formulaire et d'ouverture de pièce jointe sont semblables. L'Amérique du Sud présente une tendance particulièrement intéressante : selon l'ordre des données, les taux diminuent de gauche à droite. Le taux de clic est le plus élevé, suivi du taux de soumission de formulaire, puis du taux d'ouverture de pièce jointe; le taux de signalement est le plus faible des quatre.

Dans chaque région, le taux de soumission de formulaire était supérieur au taux d'ouverture de pièce jointe. L'ouverture de pièces jointes malveillantes peut avoir des effets très néfastes sur l'infrastructure d'une organisation en raison du risque d'infection par un virus ou un rançongiciel. On peut toutefois soutenir que la transmission d'identifiants, comme des noms d'utilisateur et des mots de passe, au moyen d'un formulaire est tout aussi dommageable.

Principales constatations

Ces données indiquent qu'il faut, dans toutes les régions, redoubler d'efforts pour apprendre aux utilisateurs à reconnaître les pièces jointes potentiellement malveillantes et les attaques visant à recueillir des identifiants.

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

2. Rendement selon la langue

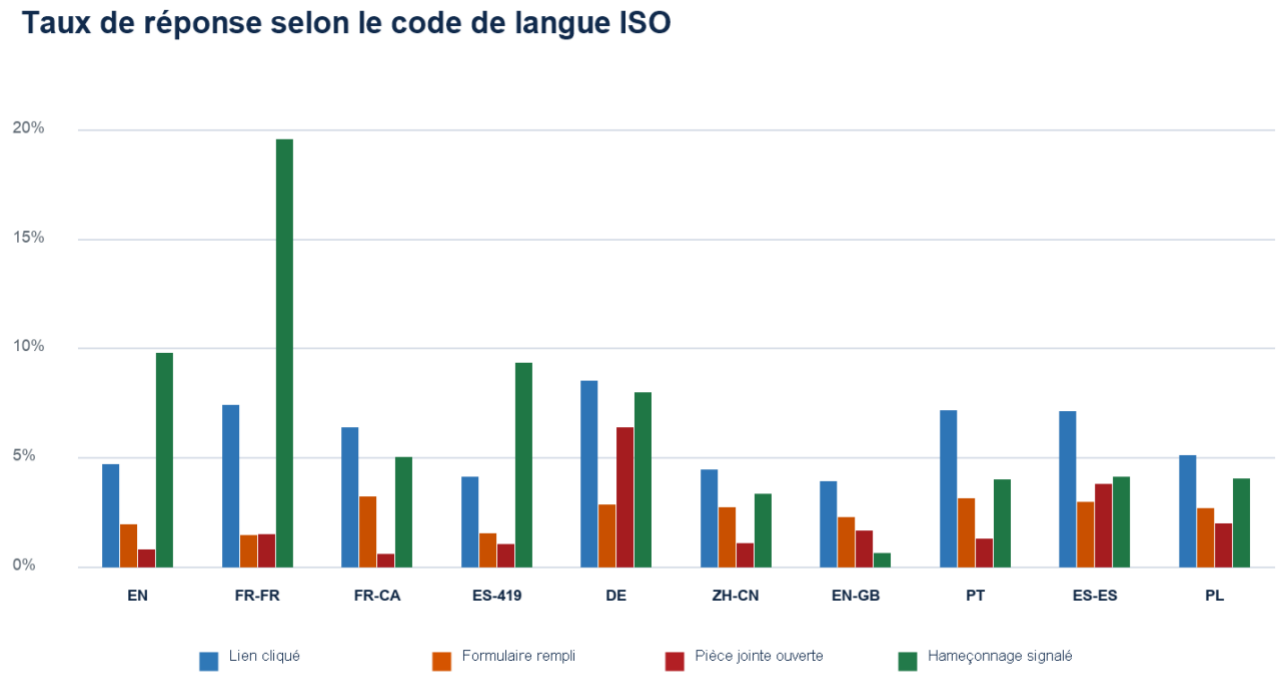

Figure 3. Taux de réponse des dix principaux groupes de codes de langue ISO selon le nombre de destinataires actifs. Voir l'annexe I, tableau 2.

Les données sur le rendement selon la langue révèlent une tendance différente de celle des données sur le risque géographique.

Dans seulement trois des dix groupes linguistiques, le taux de signalement est supérieur aux taux de clic, de soumission de formulaire et d'ouverture de pièce jointe. À titre de comparaison, cette tendance se manifeste dans trois des six régions. Le groupe EN-GB suit la même tendance que l'Amérique du Sud : son taux de clic est le plus élevé, suivi de la soumission de formulaire, de l'ouverture de pièce jointe et, enfin, du signalement, qui affiche le taux le plus faible. Le groupe FR-FR présente le taux de signalement le plus élevé, soit environ le double de celui du groupe anglais, au deuxième rang. Les taux de soumission de formulaire et d'ouverture de pièce jointe du groupe FR-FR sont presque égaux, comme dans la tendance européenne illustrée à la figure 2.

La comparaison des taux FR-FR et FR-CA est particulièrement intéressante, car leurs tendances diffèrent. Dans le groupe FR-CA, le taux de signalement est inférieur au taux de clic, à l'inverse du groupe FR-FR. Le taux d'ouverture de pièce jointe du groupe FR-CA est également inférieur au taux de soumission de formulaire, ce qui le distingue encore une fois du groupe FR-FR. Les différences entre ES-419 et ES-ES sont elles aussi dignes de mention. Le groupe ES-419 affiche un meilleur taux de signalement que le groupe ES-ES. Dans les deux cas, le taux de clic est supérieur aux taux de soumission de formulaire et d'ouverture de pièce jointe; cela vaut toutefois pour toutes les langues de la figure 3.

Principales constatations

Ces données indiquent qu'en moyenne, les utilisateurs sont plus susceptibles d'être victimes d'une attaque d'hameçonnage fondée sur la soumission d'un formulaire que d'une attaque par pièce jointe. Elles montrent aussi que, dans la plupart des langues de ce groupe, les clics sont en moyenne plus fréquents que les signalements d'hameçonnage.

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

3. Tendances selon la taille de l'entreprise

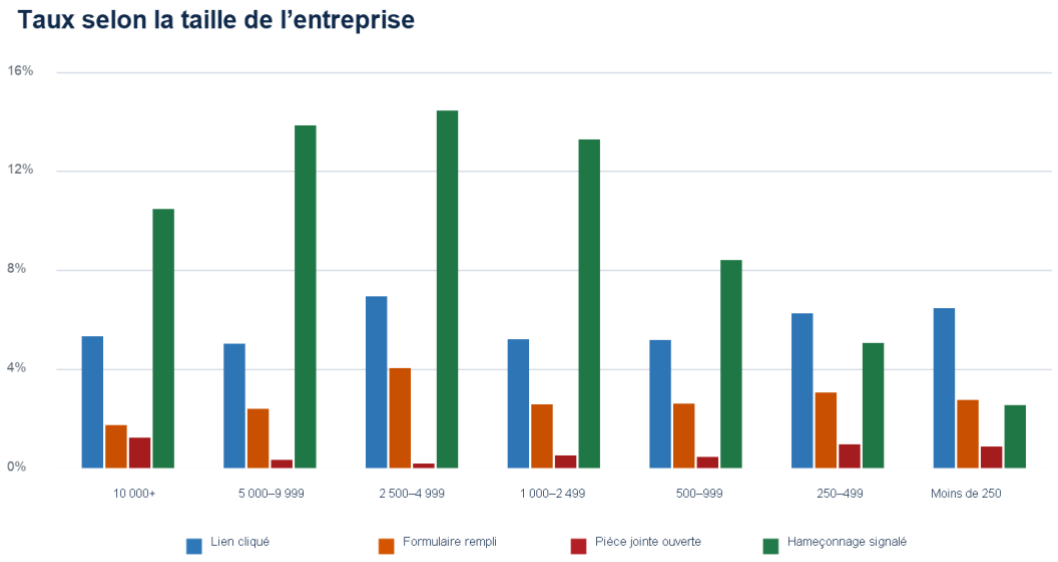

Figure 4. Taux de clic, de soumission de formulaire, d'ouverture de pièce jointe et de signalement selon la taille de l'entreprise. Voir l'annexe I, tableau 3.

L'examen des résultats des simulations d'hameçonnage selon la taille de l'entreprise permet de dégager plusieurs conclusions.

Selon Innovation, Sciences et Développement économique Canada, les entreprises sont définies comme suit :[1]

Microentreprise	1 à 4 employés
Petite entreprise	5 à 99 employés
Moyenne entreprise	100 à 499 employés
Grande entreprise	500 employés ou plus

Bien que les entreprises de 2 500 à 4 999 employés fassent figure d'exception, les petites et moyennes entreprises semblent courir le plus grand risque. Non seulement leurs taux de clic et de soumission de mot de passe sont plus élevés, mais leurs taux de signalement sont aussi les plus faibles. L'écart de signalement entre les grandes et les petites entreprises pourrait s'expliquer par les ressources disponibles. Selon le rapport 2025 sur le secteur de la formation de Training Magazine, les budgets de formation varient considérablement selon la taille de l'organisation :[2]

Petites entreprises	100 à 999 employés	**333 305 $**
Moyennes entreprises	1 000 à 9 999 employés	1 628 415 $
Grandes entreprises	10 000 employés ou plus	11 698 715 $

Fait intéressant, les plus grandes entreprises, soit celles qui comptent 10 000 employés ou plus, sont les plus susceptibles d'ouvrir les pièces jointes de courriels d'hameçonnage. La nature du travail de ces employés les a-t-elle amenés à ouvrir plus librement les pièces jointes?

[1] https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2025
[2] https://trainingmag.com/2025-training-industry-report/

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

4. Tendances sectorielles

Figure 5. Secteurs affichant les taux les plus élevés de clic, de soumission de formulaire, de signalement et d'ouverture de pièce jointe. Voir l'annexe I, tableau 4.

Les données présentées ici inspirent à la fois espoir et inquiétude. Du côté positif, près de 31 % des employés du secteur bancaire et 25 % des employés du secteur de la défense ont signalé les tentatives d'hameçonnage. Ces résultats sont nettement supérieurs à la moyenne de 10,5 % pour l'ensemble des secteurs et sont particulièrement importants compte tenu du rôle essentiel de ces secteurs.

Les statistiques des secteurs du jeu et de l'assurance sont plus préoccupantes. Plus de 16 % des employés du secteur du jeu étaient disposés à saisir leur mot de passe sur des pages d'hameçonnage. Ce résultat est presque aussi alarmant que celui du secteur de l'assurance, où plus de 12 % des employés ont ouvert des pièces jointes.

Principales constatations

Bien que les taux de clic soient préoccupants, les conséquences possibles de la saisie d'un mot de passe ou de l'ouverture d'une pièce jointe sont beaucoup plus graves. Il est impératif que les employés prennent ces menaces au sérieux. Les secteurs mentionnés ci-dessus auraient intérêt à revoir leurs formations et leurs mesures de contrôle afin d'améliorer leurs résultats l'an prochain.

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

Principaux constats

Rapport comparatif 2025 sur les simulations d'hameçonnage

Ce que les données indiquent pour les priorités de sensibilisation à la sécurité

Les résultats comparatifs doivent orienter des actions ciblées, plutôt que servir de simple bilan annuel.

La valeur du rapport ne réside pas dans un seul taux global; elle se trouve dans les tendances observées selon les signalements, les clics, les formulaires remplis et les pièces jointes ouvertes.

1

L'écart de signalement demeure central

Un taux de signalement de 10,5 % est utile, mais la plupart des simulations d'hameçonnage ne sont toujours pas signalées.

2

Le risque varie selon le segment

La région, la langue, la taille de l'entreprise et l'industrie révèlent chacune des faiblesses différentes.

3

Regarder au-delà des clics

Les formulaires remplis et les pièces jointes ouvertes sont plus risqués que les clics seuls.

4

Les petites organisations ont besoin de soutien

Les faibles taux de signalement indiquent des lacunes de ressources et de formation.

5

Adapter la stratégie avec les données

Utilisez les tendances du rapport pour prioriser la sensibilisation, les contrôles et l'accompagnement ciblé.

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.

Annexe I – Données brutes

1. Tendances géographiques du risque

Région	Clic	Formulaire	Pièce jointe	Signalement
Amérique du Nord	4,16 %	1,71 %	0,39 %	10,91 %
Europe	7,00 %	2,31 %	1,89 %	10,22 %
Asie	4,25 %	2,08 %	0,07 %	9,30 %
Afrique	6,95 %	3,74 %	0,28 %	0,65 %
Amérique du Sud	7,98 %	5,27 %	2,65 %	1,35 %
Moyen-Orient	4,20 %	2,03 %	0,00 %	0,00 %

2. Rendement selon la langue

Code de langue	Destinataires	Proportion	Clic	Formulaire	Pièce jointe	Signalement
EN	7,66 M	55,03 %	4,66 %	1,91 %	0,75 %	9,75 %
FR-FR	2,51 M	18,06 %	7,37 %	1,42 %	1,45 %	19,55 %
FR-CA	1,25 M	9,01 %	6,36 %	3,17 %	0,56 %	4,98 %
ES-419	957,5 k	6,88 %	4,09 %	1,52 %	1,02 %	9,30 %
DE	214,7 k	1,54 %	8,51 %	2,80 %	6,36 %	7,95 %
ZH-CN	198,8 k	1,43 %	4,44 %	2,70 %	1,06 %	3,30 %

3. Tendances selon la taille de l'entreprise

Taille de l'entreprise	Clic	Formulaire	Pièce jointe	Signalement
10 000 et plus	5,32 %	1,73 %	1,22 %	10,45 %
5 000 à 9 999	5,00 %	2,39 %	0,30 %	13,82 %
2 500 à 4 999	6,92 %	4,02 %	0,15 %	14,42 %
1 000 à 2 499	5,18 %	2,55 %	0,50 %	13,26 %
500 à 999	5,16 %	2,60 %	0,42 %	8,38 %
250 à 499	6,24 %	3,05 %	0,93 %	5,05 %
Moins de 250	6,44 %	2,75 %	0,84 %	2,53 %

4. Tendances sectorielles

Secteur	Clic	Formulaire	Pièce jointe	Signalement
Défense	13,02 %	3,65 %	0,00 %	24,83 %
Assurance	12,76 %	2,02 %	12,65 %	0,43 %
Services financiers – Banques	5,21 %	0,37 %	0,22 %	30,98 %
Hébergement et restauration	2,99 %	0,34 %	0,00 %	22,96 %
Services	3,84 %	1,47 %	0,08 %	17,41 %
Services juridiques	3,94 %	1,70 %	0,12 %	16,50 %
Radiodiffusion et médias	8,75 %	5,62 %	0,15 %	0,00 %
Jeu	8,20 %	16,39 %	0,00 %	0,00 %

Copyright © Fortra, LLC et son groupe de sociétés. Fortra®, les logos Fortra® et les autres marques désignées sont des marques de commerce exclusives de Fortra, LLC.