Co-présenté par

FORTRA
Terranova Security®

Microsoft

GONE PHISHING TOURNAMENT™

Rapport
d'analyse comparative sur l'hameçonnage
2022

Avant-propos

Alors que le paysage des cybermenaces change rapidement, la formation en sensibilisation à la cybersécurité évolue également. La multiplication des attaques par hameçonnage, rançongiciels, maliciels et plusieurs autres techniques, placent la cybersécurité au cœur des préoccupations des organisations à travers le monde.

L'augmentation des cybermenaces explique aussi l'évolution des conversations entourant la protection des informations sensibles. Elles vont désormais au-delà du respect des exigences minimales de formations en sensibilisation internes, sectorielles ou réglementaires. L'objectif étant de faire de la sensibilisation à la cybersécurité non seulement une priorité, mais une partie intégrante de la culture d'une organisation.

Que vos employés travaillent au bureau ou à distance, communiquer avec eux l'importance de protéger les données de l'entreprise contre les cybercriminels est essentiel. Dans bien des cas, les statistiques comparatives tirées de simulations d'hameçonnage constituent un point de départ incontournable. Elles permettent aux leaders en sécurité d'établir les tendances existantes en ce qui a trait aux comportements des employés et d'élaborer des stratégies pour réduire les risques et renforcer la sécurité de l'information.

Microsoft est fière de co-présenter le Gone Phishing Tournament 2022 et d'avoir collaboré avec Terranova Security par Fortra à la conception du modèle d'hameçonnage utilisé pendant l'événement. L'objectif était de produire un scénario d'hameçonnage crédible s'insérant dans les activités quotidiennes des employés, tout en s'appuyant sur des exemples de courriels d'hameçonnage réels et récents fournis par Microsoft.

Terranova Security est le partenaire mondial de choix de Microsoft en matière de sensibilisation à la sécurité. Ensemble, nous nous engageons à offrir à nos clients dans le monde entier, les simulations d'hameçonnage les plus représentatives des cybermenaces actuelles et ainsi à favoriser la croissance de cultures organisationnelles orientées vers la cybersécurité.

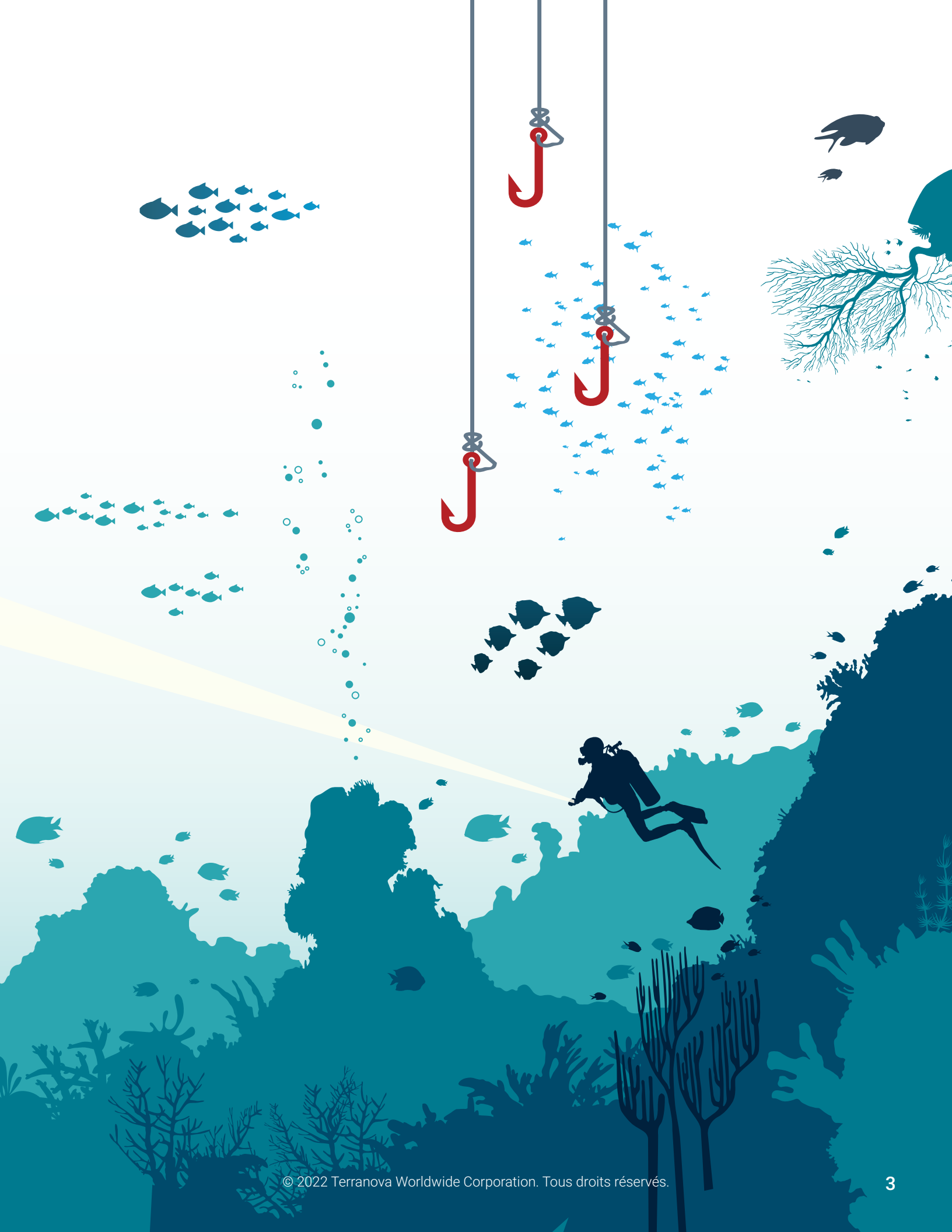


TABLE DES MATIÈRES

5 La sensibilisation à la sécurité : une culture à développer

Qu'est-ce que le Gone Phishing Tournament™ ?

6-8 Méthodologie du Gone Phishing Tournament

À propos du modèle de simulation

Stratégie de la simulation

Langues offertes pour la simulation

Aperçu des organisations participantes

9-10 Résumé des résultats

11 Comment l'hameçonnage affecte-t-il toutes les organisations ?

12 Simulations d'hameçonnage : une composante essentielle de la sensibilisation à la cybersécurité

13-21 Résultats

En résumé

Résultats par secteur d'activité : qui s'en sort le mieux ?

Résultats par nombre d'employés : à partir de quel moment la taille est-elle importante ?

Résultats par région : l'emplacement géographique des entreprises fait-il une différence ?

22-23 Comment réaliser une simulation d'hameçonnage efficace ?

L'importance de cibler des comportements par le biais de campagnes de formation fondées sur les risques

Maximiser les résultats avec des campagnes de formation à l'hameçonnage fondées sur les risques

Comment lancer des simulations d'hameçonnage efficaces ?

24 Recommandations des CISO à l'intention des employés

24 Recommandations des CISO à l'intention des responsables de la sécurité

26 À propos de Terranova Security

La sensibilisation à la sécurité : une culture à développer

La sensibilisation à la cybersécurité est désormais sur toutes les lèvres. Les cybermenaces devenant chaque jour plus complexes et omniprésentes, comprendre comment les détecter et les signaler est vital pour la productivité et la rentabilité d'une organisation. Toutefois, même avec des programmes de formation en sensibilisation à la sécurité en place, les employés continuent de cliquer sur des liens malveillants, de télécharger des pièces jointes suspectes ou de compromettre des informations sensibles.

Pourquoi?

Parce que la sécurité n'est pas complètement partie intégrante de la culture organisationnelle des entreprises. La protection des entreprises doit passer par un changement plus profond des mentalités face aux cybermenaces. Les jours où l'on pouvait simplement déployer une formation en cybersécurité pour offrir aux employés le soutien dont ils avaient besoin pour protéger les données et les systèmes sont révolus. L'indicateur le plus pertinent de la réussite d'une formation en sensibilisation est de savoir si elle peut favoriser l'adoption d'une approche orientée sur la sécurité de tous les employés, et ce dans leurs activités quotidiennes.

Le rapport 2022 sur la culture cyber, produit en collaboration avec la firme de recherche Ipsos, révèle que de nombreuses organisations ont encore beaucoup de chemin à faire pour atteindre ce niveau de sensibilisation. Aux États-Unis seulement, 35 % des employés ont exprimé peu d'inquiétude quant au vol de données au travail. De plus, 76 % d'entre eux estiment que la protection des informations de l'organisation est un rôle qui revient au service des TI.

Malgré ces lacunes, les employés demeurent la première ligne de défense contre les cyberattaques. Plus important encore, ils ont soif d'apprentissage et de développement, et c'est là où les simulations d'hameçonnage basées sur des exemples réels sont importantes. En permettant à chacun d'apprendre à identifier les signaux d'alerte des cybermenaces dans un environnement sécuritaire, les leaders en sécurité peuvent permettre à tous les employés d'apprendre par la pratique et ainsi de devenir des cyberhéros de la sécurité.

Qu'est-ce que le Gone Phishing Tournament™?

Le Gone Phishing Tournament (GPT) est un événement annuel gratuit sur la cybersécurité qui permet aux organisations à travers le monde de renforcer leurs programmes de formation en sensibilisation à la sécurité grâce à une analyse comparative détaillée. Les informations générées par ces données aident les responsables de la sécurité et de la gestion du risque à mieux comprendre les vulnérabilités de leur organisation en matière d'hameçonnage comparativement à leurs pairs, à établir des objectifs concrets de cybersécurité et à maximiser leur retour sur investissement.

L'édition 2022 de cet événement a une fois de plus profité du partenariat entre Terranova Security et Microsoft. Les deux organisations ont collaboré au développement du modèle de courriel utilisé lors de la simulation d'hameçonnage, en s'appuyant sur les renseignements recueillis par Microsoft pour représenter avec précision une vraie cybermenace.

Méthodologie du Gone Phishing Tournament

Le GPT a lieu une fois par année et est ouvert à tous les responsables en sécurité et à leurs organisations. L'édition 2022 regroupait autant des clients existants de Terranova Security que des participants sans aucun lien avec l'entreprise.

Cette simulation d'hameçonnage déployée à l'échelle mondiale a comme objectif de mesurer et d'évaluer les comportements des employés face à des menaces d'hameçonnages réalistes. Au lieu d'estimer la performance à partir de différents scénarios, comme présenté dans d'autres rapports similaires sur la sensibilisation à la cybersécurité, le GPT utilise une simulation d'hameçonnage unique pour toute la durée de l'événement. Cette uniformité permet de mesurer les taux de clic et les actions faites par les employés testés sur la base d'une même menace d'hameçonnage simulée.

Cette section présente les détails de la méthodologie utilisée pour le GPT, de l'information sur la simulation et un aperçu des participants et de la stratégie globale de l'événement.

À propos du modèle de simulation

Microsoft a fourni les modèles de courriel et de page Web utilisés cette année. Le scénario reproduisait une situation réaliste avec laquelle tous les utilisateurs sont familiers : l'arnaque de la carte-cadeau. Sélectionné par l'équipe de direction de Terranova Security, ce modèle de courriel permet d'évaluer plusieurs comportements, dont ceux de cliquer sur un lien dans un courriel d'hameçonnage, et de saisir ses données d'identification dans un formulaire sur une fausse page Web.

Les experts de Terranova Security ont évalué le niveau de difficulté du modèle de moyen à élevé. Cette évaluation est basée sur le nombre d'indicateurs d'hameçonnage et sur la difficulté d'identification des différents signaux d'avertissements.

Le courriel et la page Web ont été conçus pour imiter en tous points l'apparence d'une des nombreuses offres de carte-cadeau transmises par courriel. Pour ajouter un niveau de complexité, le message dans le courriel indiquait que la carte-cadeau serait livrée une fois que le récipiendaire aurait rempli un court questionnaire d'une question.

Stratégie de la simulation

Le GPT 2022 a eu lieu du 17 au 28 octobre. Pendant tout le processus, Terranova Security a opéré avec les contrôles de sécurité des données de sa plateforme de sensibilisation à la cybersécurité.

Si les utilisateurs cliquaient sur le lien dans le courriel de simulation d'hameçonnage, ils étaient redirigés vers une page de renvoi les invitant à saisir des informations d'identification qui, si la simulation avait été une attaque réelle, auraient été compromises. Les utilisateurs ayant complété cette deuxième étape recevaient alors une page de rétroaction présentant les indices qui auraient dû être repérés ainsi que les meilleures pratiques qui auraient dû être respectées dans une telle situation.

Après le tournoi, l'équipe de Terranova Security s'est penchée sur l'analyse des données recueillies lors de l'événement. Toutes les données des participants ont été rendues anonymes, et une fois l'analyse complétée, toutes les informations utilisées pendant le processus ont été supprimées, assurant ainsi l'entière confidentialité et sécurité des organisations participantes.

Le succès de l'événement est assuré lorsque les organisations participantes sont en mesure d'obtenir un portrait précis du taux de clics de leurs employés et de se comparer à leurs pairs.

Langues offertes pour la simulation

Pour offrir une expérience inclusive aux organisations participantes, le modèle du GPT 2022 a été offert dans encore plus de langues que l'année précédente, soit 21 au total, y compris :

- Allemand
- Anglais
- Anglais (Royaume-Uni)
- Cantonais (Hong Kong)
- Coréen
- Espagnol (Espagne)
- Français (Canada)
- Français (France)
- Grec
- Hébreux
- Hongrois
- Italien
- Japonais
- Mandarin (RPC*)
- Polonais
- Portugais (Brésil)
- Portugais (Portugal)
- Thaï
- Turc
- Ukrainien
- Vietnamien

Aperçu des organisations participantes

Le GPT 2022 a été le plus important de l'histoire de Terranova Security.

Plus de 250 organisations et 1,2 million d'utilisateurs ont participé à l'événement de cette année, ce qui en fait l'une des plus imposantes simulations d'hameçonnage en son genre. L'augmentation de la demande pour participer à cette simulation mondiale souligne à quel point les organisations prennent la sensibilisation à l'hameçonnage au sérieux à la lumière de la complexité croissante et de la prévalence accrue des menaces.

Représentation par secteur d'activité

Comme lors des années précédentes, le GPT a accueilli des organisations de toutes les tailles et de tous les secteurs. Cette année, le secteur des technologies de l'information était le plus représenté, suivi des finances, de l'éducation et du secteur public.

L'existence et la nature des programmes de formation en sensibilisation à la sécurité de chacune au sein des entreprises participantes variaient également considérablement en fonction du secteur.

Les secteurs de l'énergie, des finances, des soins de santé et du secteur public étaient ceux où l'on retrouvait le plus de programmes de formation intégrant des cours de sensibilisation à la cybersécurité et des simulations d'hameçonnage, soit la meilleure combinaison possible. Les secteurs des technologies de l'information et de l'éducation se situaient à l'autre bout du spectre, avec seulement 37 % et 38 % des organisations participantes respectivement utilisant les deux options.

Un signe encourageant pour les responsables de la sécurité est la diminution du nombre d'organisations sans programme de formation. Par exemple, 33 % des organismes à but non lucratif ont déclaré n'avoir aucun programme de formation en sensibilisation à la sécurité. Bien que ce ne soit pas idéal, cela représente tout de même une diminution importante par rapport à la proportion de 60 % dans l'édition 2021 de ce rapport.

Seuls deux secteurs — les finances et les produits de consommation, comptaient moins de 10 % d'organisations sans aucun programme de formation en sensibilisation à la sécurité, soit 6 % et 7 % respectivement.

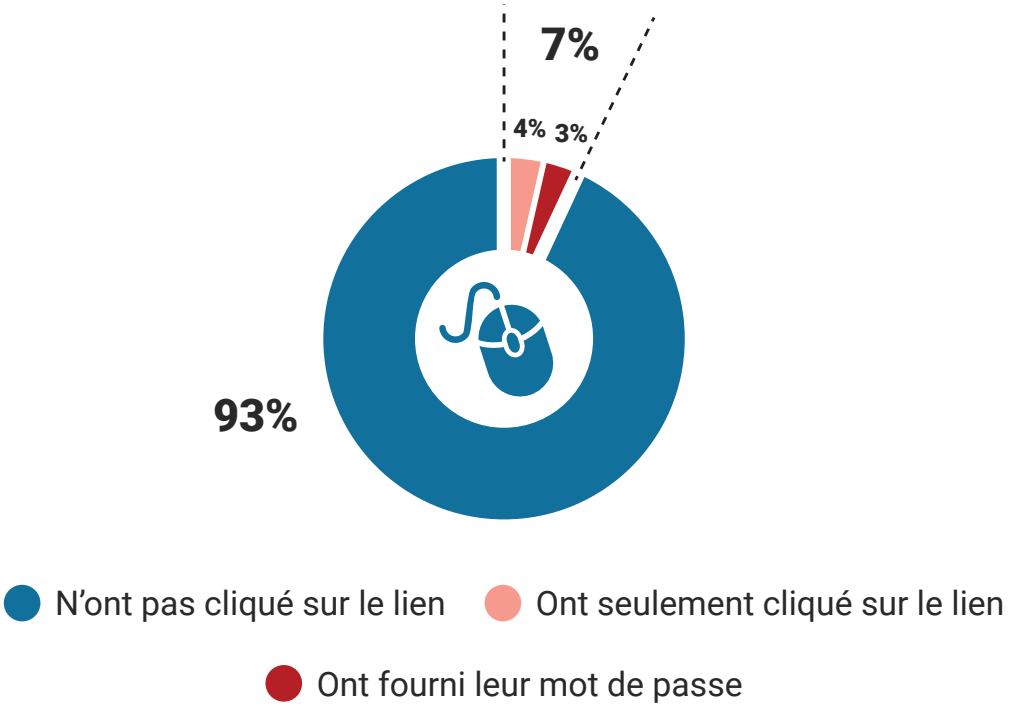
Résumé des résultats

Les résultats du GPT 2022 ont révélé que beaucoup d'utilisateurs sont toujours enclins à donner suite aux demandes concernant l'envoi de données sensibles, même si elles proviennent d'un expéditeur inconnu ou suspect.

7 %[1] des participants de la simulation ont cliqué sur le lien contenu dans le message d'hameçonnage. Ce résultat constitue une amélioration marquée par rapport aux taux de clics des éditions 2021 et 2020. Cette dernière est particulièrement intéressante puisque la simulation de cette année évaluait également le comportement des utilisateurs dans des situations d'escroquerie visant la collecte des données d'identification.

En général, seuls 3 % de tous les participants n'ont pas réussi à reconnaître la page Web d'hameçonnage et ont inscrit leurs données d'identification dans le formulaire. Cette statistique représente également une amélioration significative lorsqu'on la compare aux résultats de 2021 et 2020. En effet, lors de ces éditions, respectivement 14,4 % et 13,4 % des utilisateurs avaient effectué une action qui aurait compromis des informations sensibles si la simulation avait été une vraie cyberattaque.

RÉPONSES TOUS UTILISATEURS



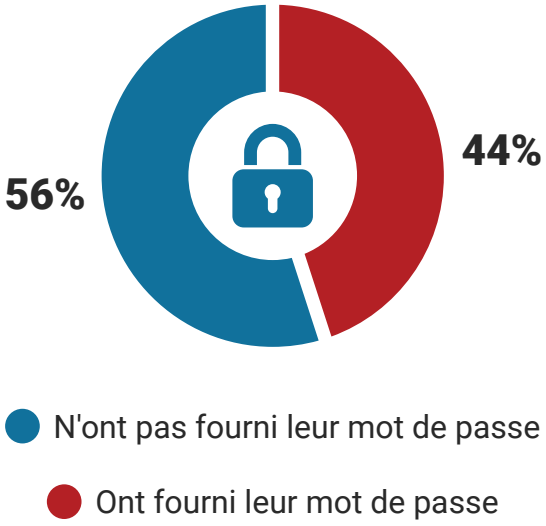
[1] *Les moyennes dans cette section de résumé sont calculées sur la base du nombre total de participants. Pour calculer cette moyenne, Terranova Security a agrégé les données de tous les participants ayant cliqué et soumis leurs informations dans le formulaire.*

Malgré cela, le ratio clic/formulaire complété représente toujours une source de préoccupation. Au total, **44 % des personnes qui ont cliqué sur le lien dans le courriel de simulation ont rempli le formulaire sur la page Web**. Encore plus inquiétant : seules les organisations comptant 500 employés et moins ont enregistré un ratio de moins de 30 %.

Ces résultats soulignent l'importance de construire un programme de formation en sensibilisation à la cybersécurité, proposant des exercices pratiques et concrets, comme les simulations d'hameçonnage. Les solutions techniques, comme les pares-feux, la protection des terminaux et même les boutons de signalement de l'hameçonnage dans les courriels ne suffisent pas à garantir la sécurité de l'information.

Il revient aux employés d'approfondir leurs connaissances en matière de cybersécurité. Ils seront ainsi en mesure de renforcer la première ligne de défense des organisations, qui est aussi la plus importante, contre les pirates informatiques.

RÉPONSES AU SITE WEB D'HAMEÇONNAGE



Qu'est-ce que le ratio clic/formulaire complété ?

Le ratio clic/formulaire complété représente le pourcentage de participants ayant réalisé les deux comportements mesurés par la simulation d'hameçonnage. Toutefois, nous n'avons pas d'information concernant les participants n'ayant pas cliqué. Peut-être n'ont-ils jamais vu le courriel d'hameçonnage ou n'y ont-ils pas réagi. Le ratio clic/formulaire complété mesure l'action causale consistant à soumettre des informations d'identification après avoir cliqué, ce qui met en évidence la décision à laquelle les utilisateurs ont été confrontés : soumettre des données sur un formulaire ou non. Ceux qui n'ont pas soumis de données ont donc pu identifier la page Web d'hameçonnage.

Comment l'hameçonnage affecte-t-il toutes les organisations ?

Une attaque d'hameçonnage réussie peut causer des dommages financiers autant à l'organisation qu'à ses clients, ses fournisseurs et ses investisseurs. Elle peut également entacher la réputation de l'organisation d'une manière irréversible en affectant la confiance des consommateurs quant à sa capacité à protéger leurs données.

Toutes ces conséquences peuvent découler d'un courriel semblant légitime, comme celui utilisé dans la simulation du GPT 2022. En raison de l'augmentation du travail à distance et des changements majeurs dans les habitudes de navigation des travailleurs, une fuite de données accidentelle peut résulter d'un seul compte ou mot de passe compromis.

Les impacts négatifs peuvent être généralisés si une organisation omet de mettre en place un programme de formation en sensibilisation à la cybersécurité qui comprend du contenu pratique et interactif, comme les simulations d'hameçonnage. Les niveaux de risque accrus dus à l'erreur humaine peuvent décourager les investisseurs et les partenaires externes de s'associer à une marque qu'ils jugent plus sensible aux cybermenaces. Par conséquent, les acheteurs potentiels pourraient choisir de faire affaire avec un compétiteur.

Dans son rapport 2021 sur la cybercriminalité, l'Internet Crime Complaint Center (IC3) du FBI indique avoir reçu plus de 847 376 plaintes liées à l'hameçonnage, ce qui représente des pertes potentielles de plus de 6,9 milliards $. Malgré cela, selon le rapport 2022 sur la culture cyber d'IPSOS et de Terranova Security, 52 % des employés considèrent toujours que leur emploi n'a aucun lien avec la cybersécurité.

Associez cette réalité à l'utilisation quotidienne d'un nombre croissant d'applications et d'appareils et vous réaliserez que le facteur de risque humain devrait figurer en tête des priorités de toutes les organisations, sans égard à leur secteur, à leur région ou à leur taille.

Simulations d'hameçonnage : une composante essentielle de la sensibilisation à la cybersécurité

Pour réduire les risques de cybersécurité, les organisations doivent commencer par identifier leurs services ou leurs employés les plus vulnérables. Qui sont les employés à haut risque ? Quels types de postes comportent les facteurs de risque les plus inhérents, comme l'accès à des informations sensibles et un volume élevé de courriels à traiter ? Et surtout, comment les performances lors des formations en sensibilisation à la sécurité contribuent-elles à la réduction globale du risque ?

Des milliards de courriels frauduleux sont envoyés chaque jour. Dans cette optique, il est essentiel de connaître le niveau actuel des connaissances en sensibilisation à la cybersécurité des employés et d'identifier les points d'amélioration potentielle afin de renforcer le facteur humain de la sécurité de l'information. Car même si les remparts technologiques d'une organisation sont parmi les plus efficaces, les employés demeurent trop souvent la porte d'entrée des cyberattaques. Il est de notre responsabilité d'en faire la première ligne de défense contre les violations potentielles de données. Pour évaluer adéquatement le risque, les simulations d'hameçonnage qui s'inspirent de cybermenaces les plus fréquentes, et imitent la façon dont elles ciblent les utilisateurs, constituent un bon point de départ. Ces outils permettent aux responsables de la sécurité d'évaluer l'ensemble des membres de l'équipe avec un scénario réaliste mesurant les aptitudes en cybersécurité des employés par l'entremise d'actions concrètes — comme le fait de cliquer ou non sur un lien ou une pièce jointe suspecte.

L'utilisation de ces renseignements permet aux décideurs de :

1. Réduire considérablement les niveaux de risque
2. Accroître la sensibilisation organisationnelle face aux cybermenaces les plus récentes
3. Minimiser les coûts liés à une attaque d'hameçonnage
4. Mesurer avec précision les niveaux de vulnérabilité des individus et de l'organisation
5. Réduire le sentiment de confiance des employés lorsqu'ils reçoivent des courriels, que ceux-ci soient légitimes ou non
6. Offrir aux employés des rétroactions ciblées et de la formation juste à temps
7. Augmenter le signalement et améliorer la réaction des utilisateurs aux tentatives d'hameçonnage
8. Prévoir des activités de formation sur l'hameçonnage en fonction des tâches des employés pour une pertinence accrue
9. Protéger les données confidentielles personnelles et organisationnelles
10. Bâtir une culture de cybersécurité et former des cyberhéros engagés dans la protection de l'entreprise

> **En connaissant exactement la position de l'organisation, les responsables de la sécurité aident à renforcer la protection des données !**

Résultats

La majorité des cyberattaques exploitent les émotions humaines, comme la tendance à faire confiance à une offre ou à une autre personne, pour accéder à des informations sensibles et les compromettre. Si un compte en ligne ou un mot de passe tombe entre les mains d'un cybercriminel, des données confidentielles, y compris des détails personnels et financiers, pourraient être volées ou utilisées pour d'autres activités malveillantes.

En se basant sur les informations les plus à jour fournies par Microsoft concernant les menaces d'hameçonnage, , la simulation conçue pour le GPT 2022 mesurait un comportement typique tout en maintenant un niveau de complexité élevé. Comme un seul modèle de courriel a été transmis aux participants lors de la simulation, les résultats présentés dans ce rapport sont parmi les plus universels de l'industrie.

Les sections suivantes présentent les résultats et les tendances générales, avant de ventiler les données par secteur, par taille de l'organisation et par région. Les résultats généraux et les ventilations globales et régionales — sont basés sur les taux de clics des utilisateurs afin d'assurer une pondération égale de toutes les variables. En revanche, les résultats par secteur et par taille sont basés sur les taux de clics par organisation.

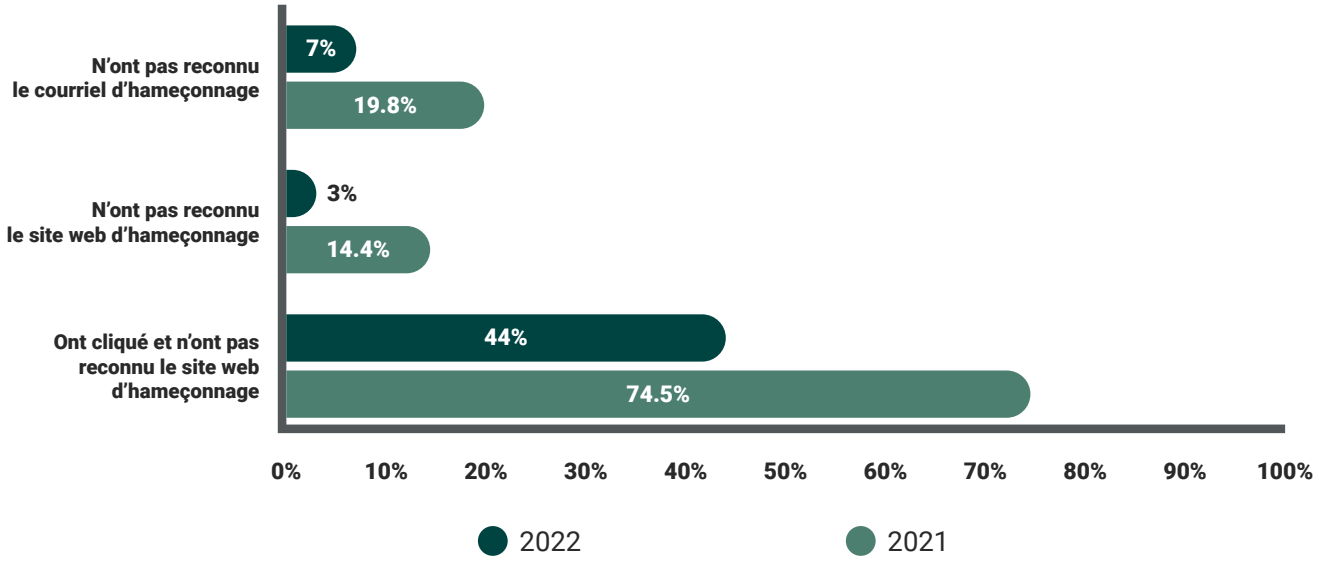
En résumé

Au total, 7 % des participants au GPT 2022 ont cliqué sur le lien du courriel d'hameçonnage, une amélioration significative par rapport aux résultats des événements de 2021 et de 2020. Tandis que 3 % de tous les utilisateurs n'ont pas reconnu les signaux d'avertissement sur la fausse page Web et y ont inscrit leurs données d'identification.

Malgré ces chiffres encourageants, le ratio clic/formulaire complété demeure trop élevé au goût de n'importe quel CISO. Au total, 44 % des personnes ayant cliqué sur le lien du courriel d'hameçonnage ont également saisi leurs données dans le formulaire sur la page Web de la simulation. De plus, seules les organisations de 500 employés et moins ont réussi à conserver leur ratio sous la barre des 30 %.

Pour mettre ces chiffres en perspective, si une entreprise de **10 000 employés** avait été la cible d'une attaque d'hameçonnage semblable à celle présentée dans le cadre de la simulation, **700 personnes auraient cliqué** sur le lien du courriel, et **308 d'entre elles auraient compromis des informations sensibles** en les partageant dans le formulaire Web.

COMPARAISON DES RÉSULTATS ENTRE 2022 ET 2021



Résultats par secteur d'activité : qui s'en sort le mieux ?

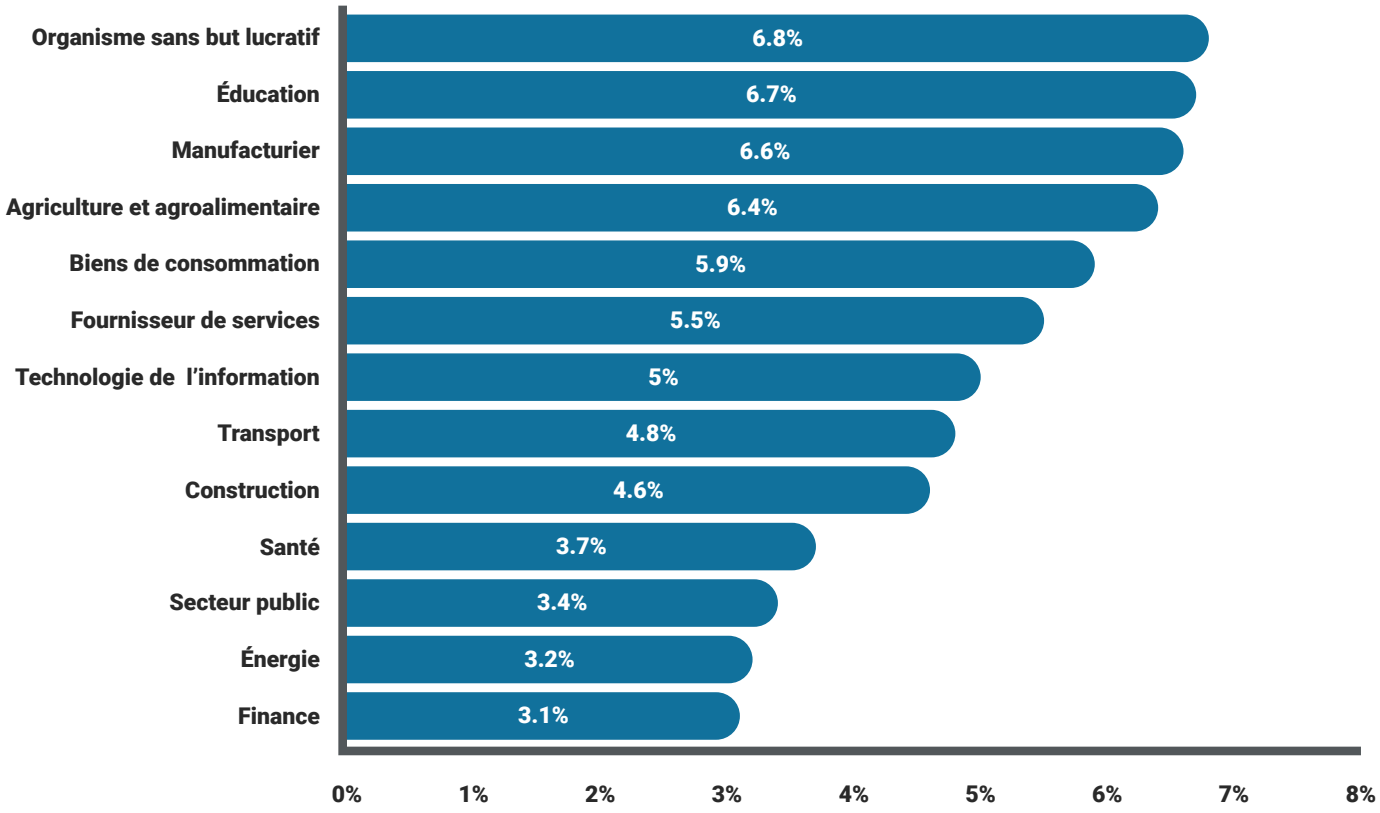
Lorsqu'on compare les taux de clics des organisations en fonction de leur secteur[2], il est important de reconnaître qu'elles ne partent pas toutes du même niveau. La diversité des normes et des exigences en matière de cybersécurité fait en sorte que les résultats aux simulations d'hameçonnage varient d'une organisation à l'autre, même si elles œuvrent dans le même milieu.

Les secteurs suivants ont affiché les taux de clics sur le lien du courriel d'hameçonnage les plus élevés :

- Organisation à but non lucratif
- Éducation
- Manufacturier
- Agriculture et agroalimentaire
- Produits de consommation

Les secteurs les plus performants en ce qui concerne les taux de clics sont la finance, l'énergie et le secteur public, qui affichent tous un résultat de moins de 3,5 %.

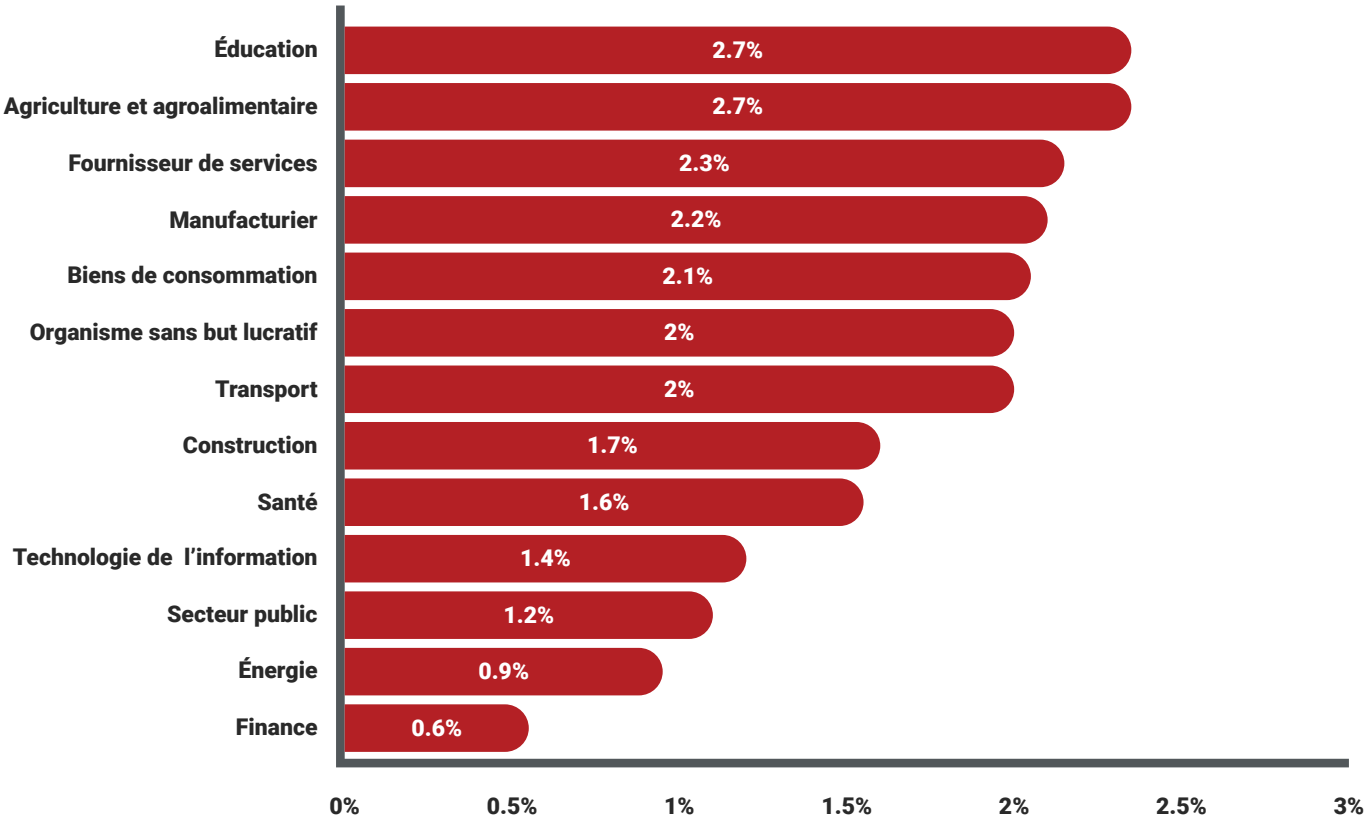
CLICS SUR LE LIEN PAR INDUSTRIE (%)



[2] *Pour calculer les moyennes par secteur d'activité et par taille d'entreprise, Terranova Security a agrégé les données des organisations participantes de chaque groupe. Ainsi, les résultats par secteur d'activité ou par taille d'entreprise sont pondérées de manière égale lors du calcul de la moyenne.*

Le secteur de l'éducation arrive également en tête pour ce qui est du taux de partage des données d'identification, avec un peu moins de 3 %. Seuls les secteurs des finances et de l'énergie ont réussi à maintenir leur taux d'envoi du formulaire en dessous de 1 %.

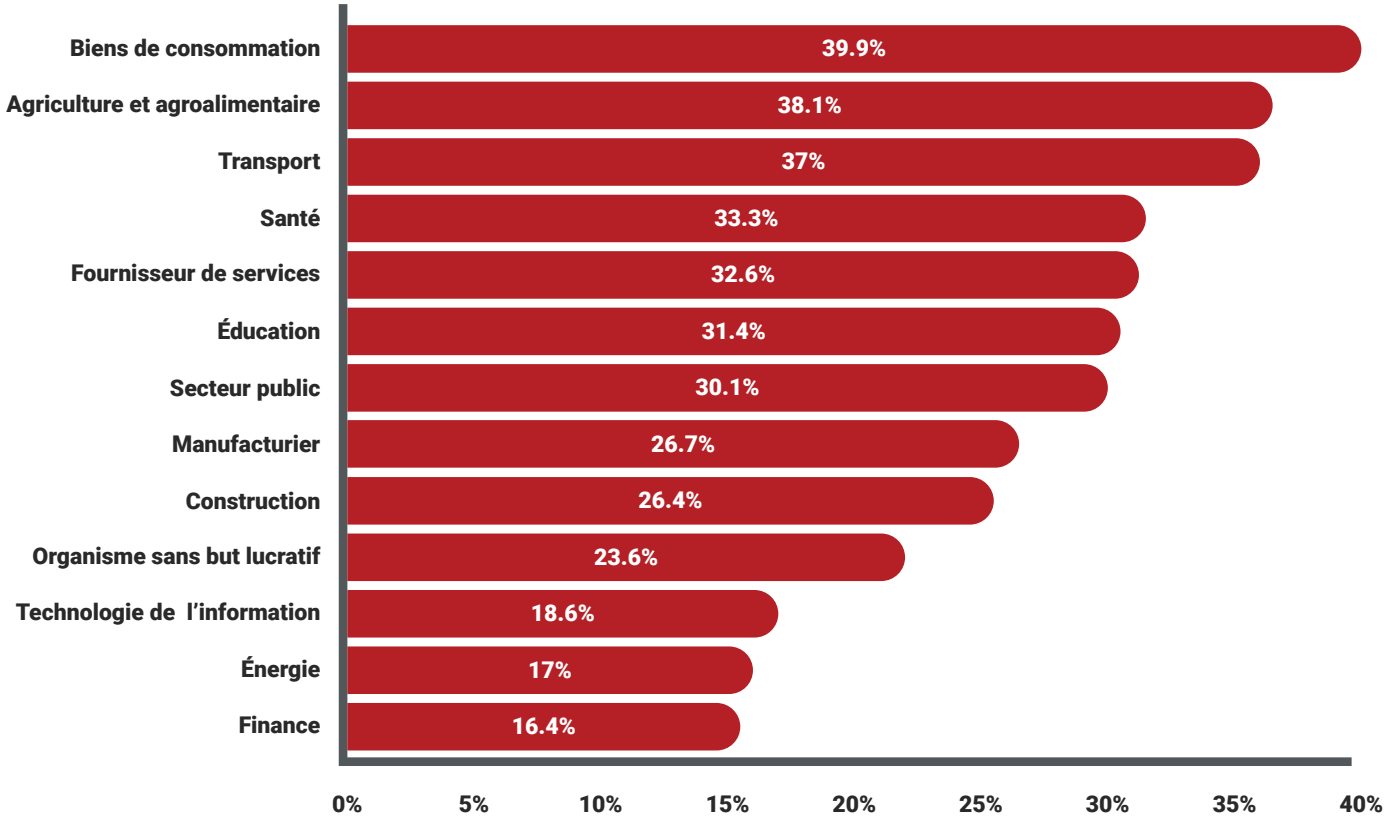
PARTAGE DU MOT DE PASSE PAR INDUSTRIE (%)



Toutefois, tout comme pour les résultats globaux du tournoi, la plus grande surprise provient des secteurs d'activité ayant enregistré le ratio clic/formulaire complété le plus élevé. Les organisations du secteur des produits de consommation ont affiché un résultat préoccupant de près de 40 %, tandis que le secteur de l'agriculture et de l'agroalimentaire suivait non loin derrière.

Les secteurs des TI, de l'énergie et des finances ont affiché une bonne performance, avec des ratios inférieurs à 20 %.

CLIC ET PARTAGE DU MOT DE PASSE PAR INDUSTRIE (%)



Ces résultats[3] soulignent que dans certains secteurs, le fait de remplir un formulaire après avoir cliqué sur un lien fait davantage partie des activités quotidiennes des utilisateurs, ce qui rend cette simulation d'hameçonnage plus pertinente en fonction des rôles. Toutefois, dans d'autres secteurs d'activités, les employés ne sont peut-être pas familiers avec les outils et fonctionnalités présentés dans la simulation, ce qui rend le courriel d'hameçonnage plus facile à repérer et à signaler.

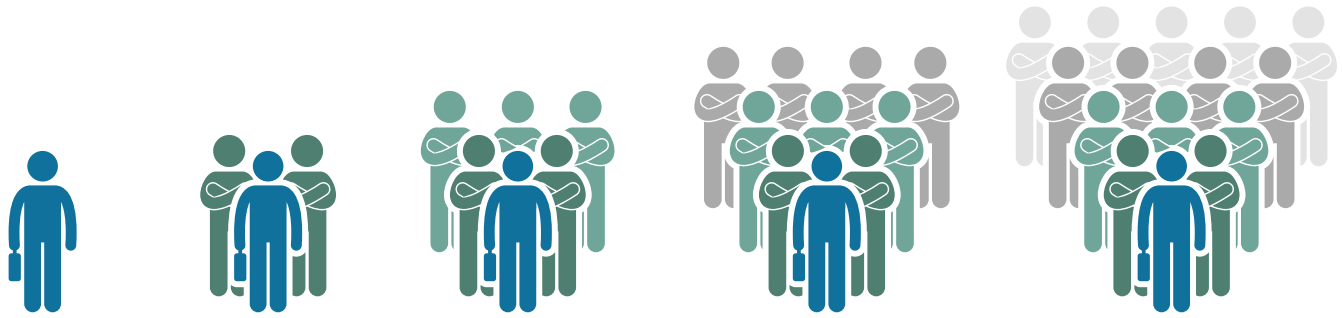
[3] *Les moyennes sectorielles peuvent différer des moyennes mondiales correspondantes, car elles sont calculées sur la base des organisations participantes plutôt que des utilisateurs participants afin de garantir une pondération égale des données.*

Résultats par nombre d'employés : à partir de quel moment la taille est-elle importante ?

Cette question est fréquemment posée dans le cadre des formations en sensibilisation à la cybersécurité. En résumé, est-ce que le fait d'allouer plus de ressources internes (budget, employés attitrés) entraîne une diminution des taux de clics de la part des utilisateurs ? La réponse est beaucoup plus complexe que « oui » ou « non ».

La simulation de 2022 montre que la taille de l'organisation influence le taux de clics et le ratio clic/formulaire complété, mais pas nécessairement de façon évidente. Les grandes organisations, qui ont typiquement accès à plus de ressources en cybersécurité que les petites organisations, ont enregistré des taux de clics totaux plus élevés. La catégorie des organisations comptant entre 3 000 et 9 999 employés a affiché le deuxième taux le plus élevé.

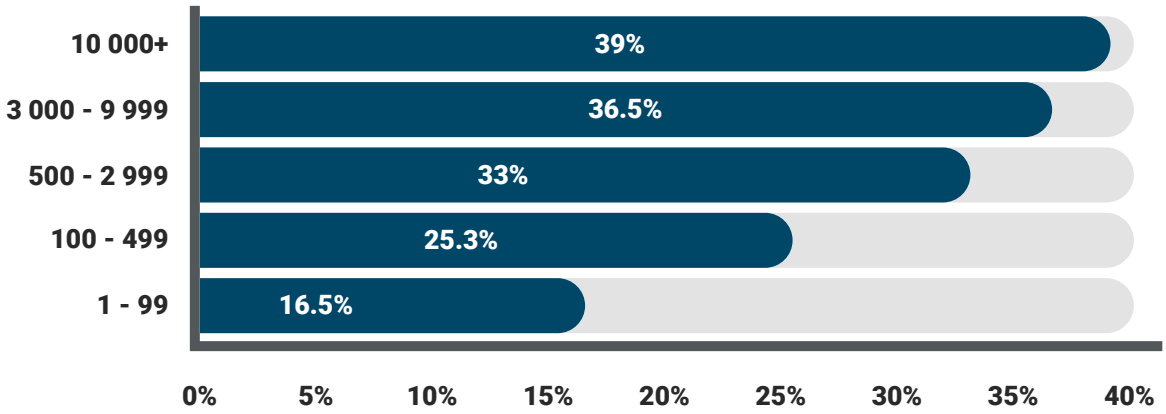
CLICS SUR LE LIEN PAR TAILLE D'ORGANISATION (%)



1 - 99	100 - 499	500 - 2 999	3 000 - 9 999	10 000+
3.6%	4.9%	5.6%	6.3%	6.9%

Les organisations comptant entre 1 et 99 employés ont obtenu les meilleurs résultats, avec un taux de moins de 3,6 %. En se focalisant sur l'extrémité supérieure de cette fourchette, cela représente environ 3 ou 4 employés ayant cliqué sur le lien du courriel d'hameçonnage. En comparant ce chiffre avec le taux de 6,9 % obtenu dans les organisations de 10 000 employés ou plus, le total des employés ayant cliqué sur le lien atteint un nombre de 690 utilisateurs.

CLIC ET PARTAGE DU MOT DE PASSE PAR TAILLE D'ORGANISATION (%)



Même si les pourcentages d'envoi des formulaires n'étaient pas très différents selon la taille des organisations, le ratio clic/formulaire complété montre tout de même des résultats révélateurs. Une fois de plus, les organisations comptant 10 000 employés et plus ont présenté le taux le plus élevé avec 39 %[4] d'employés ayant cliqué et complété le formulaire. Les entreprises comptant entre 3 000 et 9 999 employés suivaient non loin derrière, avec 36,5 %.

Ces résultats démontrent qu'une plus grande équipe ne garantit pas nécessairement de meilleures pratiques de cybersécurité. Un ratio clic/formulaire complété de 39 % dans une organisation de plus de 10 000 employés signifie que sur les 690 utilisateurs ayant cliqué sur le lien d'hameçonnage, 269 auraient compromis leurs données d'identification si la simulation avait été réelle.

Compte tenu de la taille et du volume de transactions que les organisations de ce type traitent chaque année, cette réalité devrait être plus que préoccupante pour les responsables de la sécurité.

En conclusion, la stratégie d'une organisation concernant son programme de formation en sensibilisation à la cybersécurité et l'exécution d'initiatives individuelles peuvent avoir plus d'importance que l'ampleur de ses ressources. Selon les données recueillies, bien que les organisations de 10 000 employés et plus ratent rarement une occasion de formation en sensibilisation à la sécurité, leur efficacité générale peut être remise en question. Les grandes organisations ayant souvent plus de difficultés à atteindre tous les employés lors d'activités de sensibilisation et à obtenir un taux de participation élevé.

Les grandes entreprises doivent également relever le défi supplémentaire de gérer un plus grand nombre d'employés et de les mobiliser, en particulier dans les contextes où le télétravail prime.

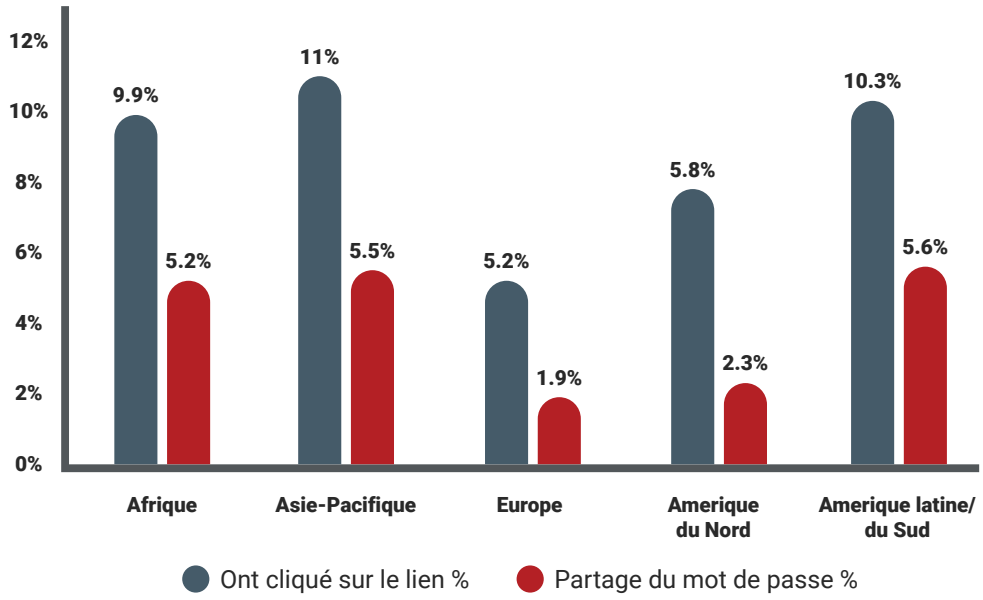
[4] *Il est normal que les moyennes par taille d'entreprises soient inférieures à la moyenne mondiale car elles sont calculées sur la base des organisations participantes et non des utilisateurs participants.*

Résultats par région : l'emplacement géographique des entreprises fait-il une différence ?

La région d'une organisation, dans la mesure où elle a un impact sur la clientèle et la localisation des employés, joue un rôle de plus en plus important dans le niveau de sensibilisation à la cybersécurité. Dans l'Union européenne, les règlements de protection des données et de conformité, comme le RGPD, peuvent influencer la façon dont une organisation recueille, stocke et manipule les données des clients, ainsi que la couverture médiatique qui est accordée aux violations de données.

Tandis que dans de nombreux secteurs, le travail à distance devient la norme, les services des TI ont une mission de plus en plus difficile : veiller à ce que tous les employés soient en mesure de reconnaître les cybermenaces et de s'en protéger. Même si les résultats[5] du GPT 2022 représentent une amélioration par rapport à ceux de 2021, ils soulignent également la complexité de naviguer dans des réalités changeantes.

CLICS SUR LE LIEN PAR RÉGION (%)

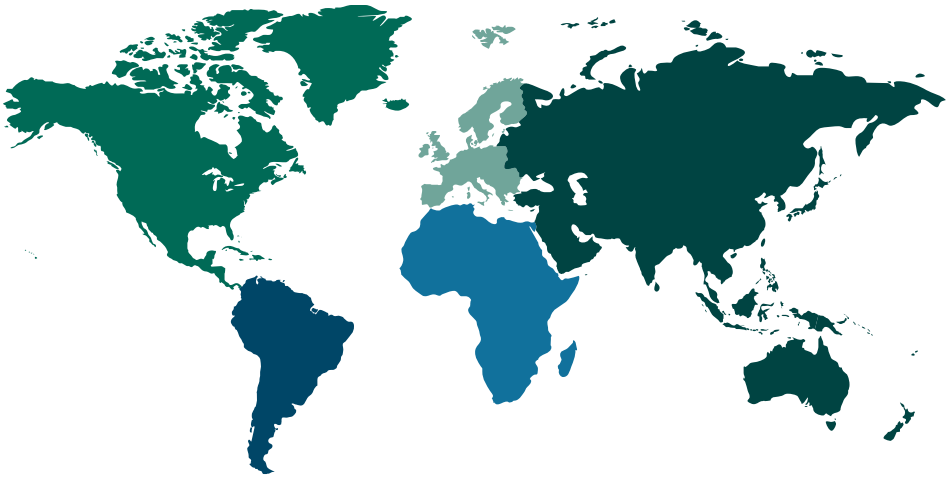


Parmi les cinq régions représentées par les participants au GPT, l'Europe a réalisé la meilleure performance, avec les taux de clics et d'envoi du formulaire les plus faibles. L'Amérique du Nord, qui avait remporté la première place en 2021, glisse en deuxième position.

Quant aux participants de la région de l'Asie et du Pacifique, ils ont enregistré le taux de clics le plus élevé. Il s'agit d'une des deux régions atteignant un résultat à deux chiffres. La région regroupant l'Amérique du Sud et l'Amérique latine a quant à elle enregistré le taux d'envoi du formulaire le plus élevé, devançant de peu les participants de la région Asie/Pacifique de 0,1 % dans cette catégorie.

[5] *Les résultats régionaux ont été calculés en fonction de l'emplacement des utilisateurs participants. Pour calculer cette moyenne, tous les utilisateurs et cliqueurs participants ont été regroupés par région en fonction de leur pays.*

CLIC ET PARTAGE DU MOT DE PASSE PAR RÉGION (%)



54%	AMERIQUE LATINE/ DU SUD
53%	AFRIQUE
50.1%	ASIE-PACIFIQUE
39.7%	AMERIQUE DU NORD
36%	EUROPE

Comme dans les éditions précédentes de l'événement GPT, ces indicateurs préliminaires ne disent pas tout. Les utilisateurs basés en Europe ont enregistré le plus faible ratio clic/formulaire complété général, tandis que les participants de l'Amérique du Sud et Latines ont présenté le résultat le plus élevé dans cette catégorie, suivis de près par l'Afrique. Le résultat de cette dernière région est d'autant plus intéressant qu'elle se classe en milieu de peloton pour les autres indicateurs régionaux.

Le ratio clic/formulaire complété relativement élevé peut être attribué à la nature réaliste de la simulation d'hameçonnage que Terranova Security a conçue pour l'événement de cette année en collaboration avec Microsoft. Les menaces d'hameçonnage évoluent constamment afin de refléter les messages que n'importe quel professionnel peut recevoir dans ses activités quotidiennes. En exploitant cette familiarité, il est beaucoup plus facile pour des cybermenaces comme celle de la simulation de passer inaperçues.

En outre, la meilleure formation en sensibilisation à la sécurité doit inclure des données récentes et les tactiques réellement utilisées par les pirates informatiques lors d'attaques d'hameçonnage réelles. Si ces éléments ne sont pas présents, l'expérience globale de l'utilisateur pourrait ne pas correspondre à la réalité des menaces actuelles. Cela aurait comme conséquence d'affaiblir la base de connaissances dont tous les employés ont besoin pour détecter et signaler systématiquement les cyberattaques potentielles.

Comment réaliser une simulation d'hameçonnage efficace ?

L'importance de cibler des comportements par le biais de campagnes de formation fondées sur les risques

De nos jours, la sensibilisation à la cybersécurité ne se résume pas simplement au déploiement de cours de formation et de simulations d'hameçonnage. Ces composantes font partie intégrante du processus, puisqu'elles ajoutent une dimension dynamique et pratique à l'apprentissage des connaissances requises en sécurité de l'information. Mais il ne s'agit que de la pointe de l'iceberg. Pour réellement renforcer la sécurité de l'information, il faut que les organisations construisent et favorisent une culture organisationnelle où les meilleures pratiques de cybersécurité demeurent en tête des priorités de tous les employés.

Pour y arriver, les responsables de la sécurité ont besoin d'information pour déterminer les niveaux de risque individuel par utilisateur ou par fonction. En évaluant les risques et en se basant sur des données, comme celles générées par l'indice de culture de sécurité développé par Terranova Security, les CISO peuvent identifier facilement les utilisateurs à haut risque, encourager les changements de comportement et renforcer la culture de cybersécurité au fil du temps. Les simulations d'hameçonnage et autres initiatives de sensibilisation à la sécurité doivent s'appuyer sur des données pour atteindre un maximum d'efficacité. Sans elles, les gains obtenus dans les campagnes de formation finissent par s'estomper.

Maximiser les résultats avec des campagnes de formation à l'hameçonnage fondées sur les risques

Une fois les bonnes données en main, les responsables de la sécurité doivent établir une stratégie de sensibilisation à la sécurité en s'appuyant sur un cadre de travail éprouvé qui permettra des changements de comportements durables. En jetant les bases d'un parcours d'apprentissage défini pour l'utilisateur, vous vous assurez que vos campagnes de formation en sensibilisation ciblent les habitudes des utilisateurs les plus souvent exploitées par les pirates.

Terranova Security a identifié sept comportements ciblés par les cybermenaces que chaque organisation devrait connaître :

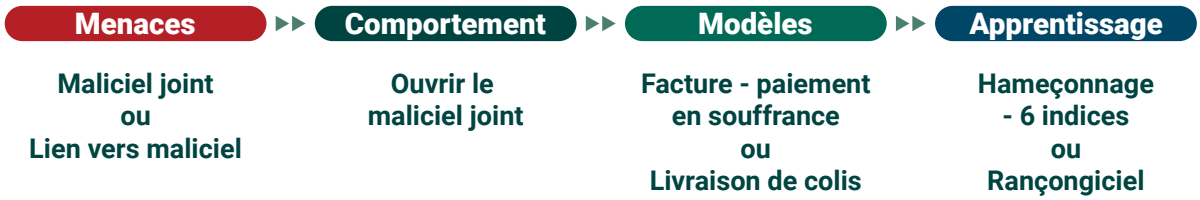
MENACES

- Logiciel malveillant en pièce jointe
- Lien vers un fichier malveillant
- Lien dans la pièce jointe
- URL malicieuse
- Collecte d'authentifiant
- Corruption de courriel professionnel

COMPORTEMENTS

- Ouvrir un fichier malveillant en pièce jointe
- Cliquer sur un lien ou un bouton
- Dévoiler un identifiant utilisateur ou un mot de passe
- Dévoiler des renseignements permettant d'identifier un employé
- Dévoiler des informations financières de l'entreprise
- Dévoiler des renseignements permettant d'identifier une personne
- Dévoiler des informations financières personnelles

Exemple de formation selon le risque



L'illustration montre le lien entre une menace donnée et le comportement de l'utilisateur qui peut compromettre les données sensibles. Selon le ou les comportements que vous souhaitez modifier, vos modules de formation et vos simulations d'hameçonnage doivent travailler ensemble pour enseigner aux employés les étapes à suivre lorsqu'ils sont confrontés à un scénario spécifique.

Une fois que votre stratégie est établie et que vous êtes prêt à lancer votre formation en sensibilisation, Terranova Security recommande d'utiliser des outils de communication pour encourager la participation de tous les collaborateurs de l'organisation. Pour lancer votre campagne de formation, commencez par une simulation d'hameçonnage général qui permettra d'évaluer le niveau de connaissance des employés.

Comme le degré de complexité des scénarios varie, les simulations d'hameçonnage que vous choisirez d'utiliser auront une influence sur le taux de clics. Si vos utilisateurs ne cliquent jamais sur le lien dans le courriel de simulation, il est possible que le scénario choisi ne soit pas assez difficile. Dans ce contexte, il convient de viser la qualité plutôt que la quantité.

Comment lancer des simulations d'hameçonnage efficaces ?

Il peut être relativement facile d'adopter une approche proactive et fondée sur les données dans le cadre d'une formation en sensibilisation à la cybersécurité. Pour éduquer les utilisateurs et changer les comportements ciblés par les cybercriminels, suivez ces directives :

1. **Ciblez les bons comportements** en étudiant vos données de cybersécurité existantes et en identifiant les tendances ou les actions particulières qui ont mené à des violations de données.
2. **Créez des simulations d'hameçonnage** qui abordent ces faiblesses et utilisez des scénarios actualisés auxquels les utilisateurs pourraient être confrontés au quotidien.
3. **Collectez des données de simulation d'hameçonnage en temps réel** pour faciliter l'évaluation, la mise à jour et le raffinement de vos initiatives de sensibilisation à la cybersécurité.
4. **Suivez et surveillez les progrès des employés** pour déterminer les niveaux de risque spécifiques aux utilisateurs et l'efficacité globale de votre démarche de sensibilisation à la sécurité.
5. **Déployez des modules de formation juste à temps** pour donner aux utilisateurs la rétroaction instantanée dont ils ont besoin en cas d'échec de la simulation d'hameçonnage.
6. **Utilisez des campagnes de formation personnalisables** basées sur vos données afin d'adapter chaque aspect du processus d'apprentissage à l'atteinte de vos objectifs.
7. **Choisissez une solution flexible et inclusive** qui propose un contenu de formation multilingue et accessible afin d'offrir aux employés une expérience d'apprentissage en ligne harmonieuse et adaptée à leurs besoins.

Recommandations des CISO à l'intention des employés

Pour éviter d'être victimes d'une attaque d'hameçonnage comme celle présentée dans le cadre de la dernière édition du GPT, les CISO de Terranova Security recommandent aux employés de toujours garder à l'esprit les bonnes pratiques suivantes :

1. **Vérifiez le nom de domaine du courriel de l'expéditeur.** Assurez-vous de donner suite uniquement aux messages provenant de sources légitimes en vérifiant les éléments de l'adresse courriel de l'expéditeur. Il est facile de ne pas remarquer le « n » supplémentaire dans « amazonn.com », surtout si le message a été conçu pour ressembler en tous points à ceux transmis par la véritable entreprise.
2. **Analysez le contenu et le ton du message.** Méfiez-vous des messages qui utilisent un ton urgent pour vous persuader d'agir immédiatement, surtout sous prétexte d'avoir gagné un concours. En règle générale, si l'offre semble trop belle pour être vraie, c'est probablement le cas.
3. **Ne transmettez jamais des informations sensibles par courriel.** Quelle que soit la nature de l'offre ou l'urgence du message, évitez de transmettre des données confidentielles en réponse à un courriel suspect. Ces informations comprennent votre nom, votre adresse, votre numéro de téléphone et vos données financières.
4. **Évitez de cliquer sur un lien contenu dans un courriel non sollicité.** Pensez-y à deux fois avant de cliquer sur un lien provenant d'un message non sollicité, ou d'une organisation ou d'un expéditeur inconnu. Passez votre curseur sur l'hyperlien pour générer un aperçu de l'URL dans votre navigateur et vérifier sa légitimité. En cas de doute, évitez de cliquer.
5. **Inspectez les sites Web avant de soumettre des données.** Une fois que vous avez cliqué sur un lien, il n'est pas trop tard pour éviter d'être victime d'une attaque. Avant de soumettre des informations sur un site Web, assurez-vous qu'il est sécurisé et qu'il appartient à une entité légitime. Vérifiez que l'URL ne contient pas de caractères ajoutés ou remplacés.

Recommandations des CISO à l'intention des responsables de la sécurité

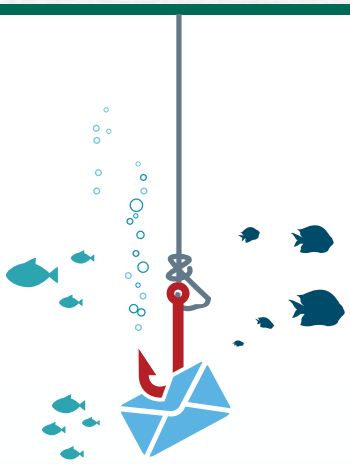
Pour vous assurer que votre organisation prend toutes les mesures nécessaires pour concevoir une campagne de formation en sensibilisation à la cybersécurité réussie, les CISO de Terranova Security conseillent de suivre les étapes suivantes :

1. **Prenez des décisions en fonction de vos objectifs et basées sur des données.** Établissez des objectifs réalistes (par exemple : réduire le taux de clics des employés de 5 points de pourcentage sur 12 mois) et développez une stratégie de sensibilisation à la sécurité qui vous permettra de les atteindre. Utilisez vos données de référence sur l'hameçonnage comme point de départ.
2. **Tirez profit d'un contenu de formation de qualité.** Priorisez le déploiement d'activités stimulantes et interactives de formation en sensibilisation à la cybersécurité afin de maximiser la participation aux cours et favoriser leurs réussites. Utilisez également du contenu, comme les jeux Serious Games de Terranova Security, pour une expérience d'apprentissage plus ludique.
3. **Adaptez les initiatives de formation pour une éducation continue.** Élaborez un programme de formation qui prévoit des activités de formation et de renforcement tout au long de l'année afin que les meilleures pratiques en matière de cybersécurité demeurent en tête des priorités à travers toutes les unités de l'organisation.
4. **Mesurez les progrès et optimisez votre stratégie.** En tenant compte de vos résultats initiaux et de vos objectifs en matière de formation en sensibilisation, assurez-vous également d'optimiser votre programme en continu. Concentrez-vous sur les points à améliorer et efforcez-vous d'offrir la meilleure expérience possible aux utilisateurs.
5. **Favorisez le développement d'une culture organisationnelle orientée vers la cybersécurité.** Prenez des mesures pour intégrer l'importance de la cybersécurité dans le quotidien des employés de votre organisation. Assurez-vous que les employés comprennent que la protection des informations sensibles est la responsabilité de tous et pas seulement du service des TI.

DÉCOUVREZ CE QUE LES EMPLOYÉS PENSENT VRAIMENT DE LA SENSIBILISATION À LA CYBERSÉCURITÉ

TÉLÉCHARGER MON RAPPORT

GONE PHISHING TOURNAMENT™



Vous avez manqué l'événement de cette année ?

Contactez-nous pour en savoir plus sur la prochaine édition du Gone Phishing Tournament. Les clients peuvent à tout moment effectuer une simulation à l'aide de l'un des modèles de courriels d'hameçonnage des précédents tournois GPT.

À propos de Terranova Security

Terranova Security par Fortra simplifie la mise en place de formations en sensibilisation à la cybersécurité et de simulations d'hameçonnage en offrant le meilleur contenu de l'industrie. Elle offre ainsi à chaque employé la possibilité de mieux comprendre l'hameçonnage, l'ingénierie sociale, la confidentialité des données, la conformité et d'autres bonnes pratiques de sécurité essentielles. Toutes nos options de formation en sensibilisation à la sécurité sont conçues pour répondre aux objectifs du client. Chaque élément de contenu et chaque modèle de simulation d'hameçonnage sont construits de façon à soutenir les objectifs des organisations en matière de cybersécurité et à renforcer leur sécurité informatique à long terme.

Terranova Security est fière de faire partie du portfolio complet de solutions de cybersécurité de Fortra. Fortra vient simplifier le paysage complexe de la cybersécurité en rassemblant des produits complémentaires afin de répondre aux enjeux de sécurité de façon innovante. Grâce à la protection puissante offerte par Terranova Security et bien d'autres, Fortra devient votre fidèle allié à chaque étape de votre parcours en cybersécurité.

Notes

GONE PHISHING TOURNAMENT™

Co-présenté par

FORTRA
Terranova Security®

Microsoft