GONE PHISHING TOURNAMENT™

2020

Rapport d'analyse comparative sur l'hameçonnage

Co-présenté par

TERRANOVA SECURITY

Microsoft

Toute personne travaillant dans des rôles de cybersécurité, de technologie ou de direction d'entreprise sait que les enjeux de protection des données confidentielles n'ont jamais été aussi élevés. De nombreuses organisations changent comment ils fonctionnent, avec le travail à distance et d'autres considérations réduisant l'efficacité moyenne de votre filet de sécurité technique. Plus que jamais, vos utilisateurs doivent savoir détecter et éviter les fraudes par hameçonnage.

Pour les organisations qui cherchent à voir comment leurs efforts de sensibilisation à la sécurité se comparent à ceux de leurs pairs, le rapport mondial d'analyse comparative sur l'hameçonnage de Terranova Security, qui s'appuie sur les résultats du plus récent Gone Phishing Tournament™, est un excellent point de départ.

Microsoft est fière de co-présenter l'édition 2020 du Gone Phishing Tournament™ et d'avoir collaboré, avec son équipe de direction, à l'élaboration du modèle d'hameçonnage utilisé lors de l'événement. L'ensemble du groupe souhaitait proposer un scénario actuel et ancré dans la vie quotidienne des utilisateurs du monde entier. Nous voulions également exploiter les données Microsoft récoltées en temps réel en ce qui a trait aux courriels d'hameçonnage et ainsi élever la qualité en matière de sensibilisation à la sécurité.

Microsoft est également reconnaissante de compter sur Terranova Security à titre de partenaire mondial de choix en sensibilisation à la sécurité ce qui nous assure d'offrir la meilleure formation possible aux clients du monde entier. Les données et les informations fournies dans ce rapport peuvent aider n'importe quelle organisation, quel que soit sa taille, son secteur d'activité ou son emplacement géographique, à renforcer son pare-feu humain et, grâce à une analyse comparative précise, à obtenir une image réelle de la façon de développer ses initiatives de formation en sensibilisation à la sécurité de manière efficace.

En responsabilisant vos employés grâce à la sensibilisation à l'hameçonnage basée sur des données concrètes, vos données organisationnelles.

Microsoft

BRANDON KOELLER

Principal Program Manager Lead - Office 365 Security

TABLE DES MATIÈRES

L'hameçonnage : Une menace plus complexe que jamais

L'année 2020 a été marquée par de grands bouleversements pour les organisations à l'échelle de la planète. Une pandémie mondiale et l'accélération de la transformation numérique ont ouvert la voie à un virage vers le travail à distance et à une « nouvelle normalité » qui, en fait, n'a rien de normal. Ces transformations ont également élevé considérablement le niveau de cybermenaces, puisque les fraudeurs en ligne du monde entier ont profité du contexte extrêmement volatile en organisant des attaques d'hameçonnage ciblées.

Les cybercriminels savent bien que de nombreux travailleurs doivent s'ajuster à un nouvel environnement de travail, plus précisément à un bureau à la maison. Les utilisateurs sont plus vulnérables à des courriels, des appels ou des SMS d'hameçonnage soigneusement préparés, ainsi qu'à d'autres formes de cyberattaques. Les cybercriminels profitent du climat de crainte et d'incertitude instauré par cet événement mondial pour leurrer les utilisateurs et compromettre leurs systèmes et leurs informations.

De janvier à mars 2020 seulement, on a vu une augmentation ahurissante de 30 000 % (non, ce n'est pas une erreur de frappe) du nombre de messages suspects ayant ciblé des travailleurs à distance. Le nombre d'attaques d'hameçonnage ou de harponnage associées à la COVID-19 s'est également accru de 667 %. Selon Microsoft, sur les millions de courriels d'hameçonnage vus et suivis chaque jour, environ 60 000 comprennent des fichiers joints ou des URL malveillants associés à la COVID-19.

Le coût moyen d'une brèche de données est passé à 137 000 $, ce qui a placé toutes les organisations face à beaucoup plus d'enjeux qu'auparavant. En effet, tout part avec un seul utilisateur qui se prend dans les filets d'un courriel, d'une page web ou d'un téléchargement malveillant pour compromettre d'immenses quantités de données confidentielles.

La première étape d'un programme efficace de sensibilisation à la sécurité et à l'hameçonnage est de comprendre où votre organisation se situe. Pour établir un point de référence précis se basant sur de réelles menaces d'hameçonnage, Terranova Security a déployé la deuxième édition de son Gone Phishing Tournament.

En quoi consiste le Gone Phising Tournament™?

Cet événement annuel en cybersécurité recueille des données représentatives sur la sensibilisation à l'hameçonnage, afin de générer de puissantes connaissances. Celles-ci sont mises à profit par les responsables de la sécurité et de la gestion du risque pour mieux comprendre le risque qui pèse sur leur organisation. Le tournoi représente également le point de départ du parcours de sensibilisation à la sécurité des organisations, et il peut aider à établir des objectifs plus concrets.

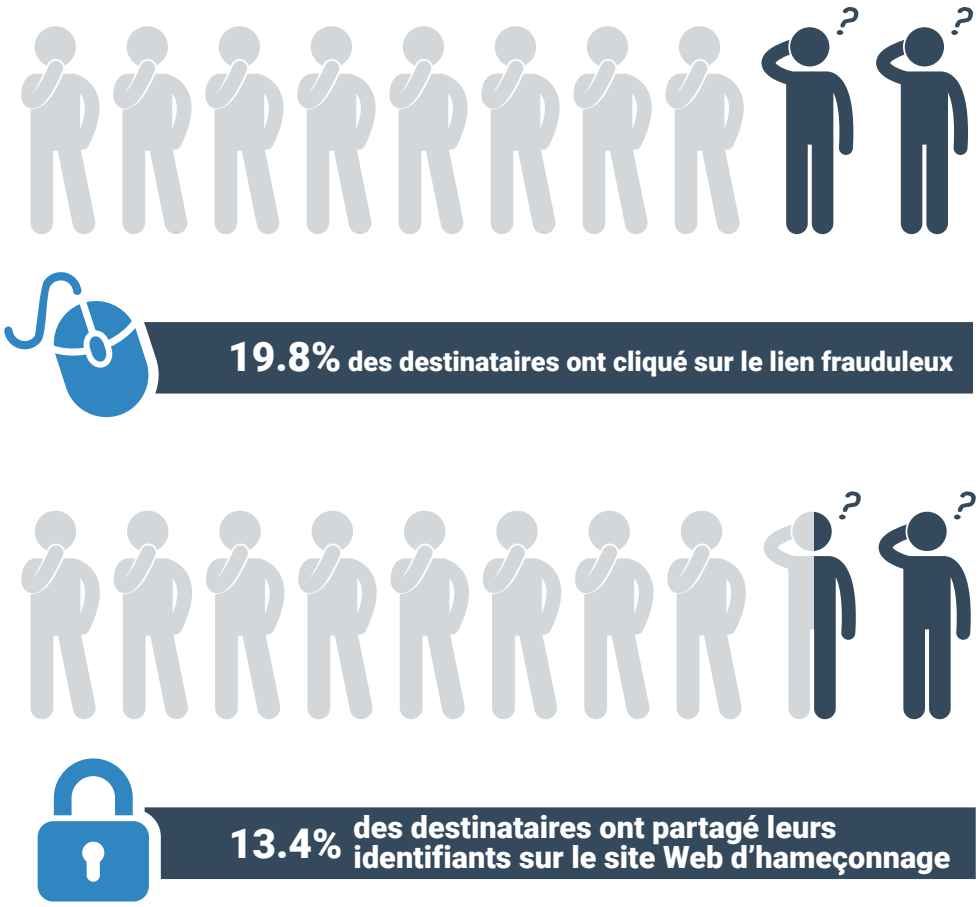
Cette édition du Gone Phishing Tournament™ a également bénéficié du partenariat entre Terranova Security et Microsoft. La simulation d'hameçonnage est le résultat d'une collaboration entre les deux organisations. Nous avons donc utilisé l'intelligence en temps réel de Microsoft pour concevoir de façon précise le contexte d'une simulation d'hameçonnage telle que les utilisateurs sont susceptibles d'en vivre dans leur quotidien.

ALORS, COMMENT VOTRE TAUX DE CLICS SE COMPARE-T-IL?

Sommaire des constats

La deuxième édition du Gone Phishing Tournament s'est déroulée sur 11 jours, en octobre 2020. Des organisations et des utilisateurs de partout dans le monde ont participé à l'événement qui a mis en lumière les lacunes en matière de sensibilisation à l'hameçonnage.

Le Gone Phishing Tournament de 2020 a révélé que près de 20 % des employés sont encore prompts à cliquer sur les liens joints à des courriels d'hameçonnage, même lorsque leur organisation a déjà en place un programme de sensibilisation à la sécurité ou aux risques de l'hameçonnage. Les résultats sont préoccupants, surtout que le tournoi s'est tenu durant le Mois de la sensibilisation à la cybersécurité, où les activités d'apprentissage et les communications entourant l'hameçonnage et des sujets connexes sont pourtant en hausse.



De plus, la plupart des organisations qui ont font une simulation d'hameçonnage pour la première fois observent un taux de clics de 20 % à 30 %, et un taux de divulgation de données en ligne de 10 % à 15 % (en moyenne, 50 % des cliqueurs divulguent des données via des formulaires en ligne). La majorité des participants au tournoi avaient déjà en place un programme de simulation d'hameçonnage, et ne devraient donc pas démontrer un taux de clics aussi élevé.

Une fois que ces personnes ont cliqué, la grande majorité a poursuivi une tendance dangereuse.

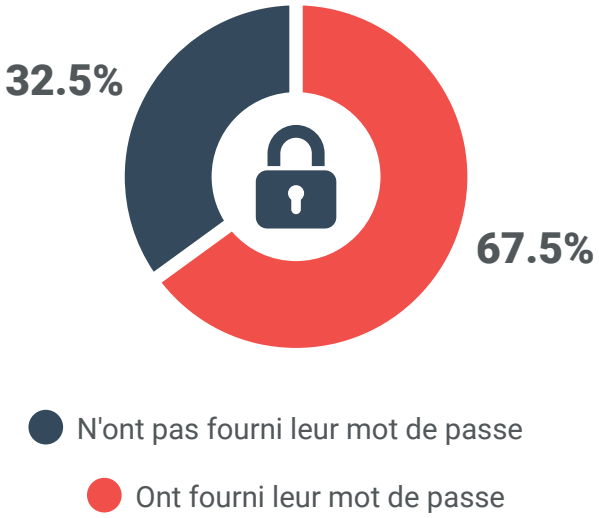
Plus de 67 % (figure 1) des cliqueurs ont entré leurs identifiants sur une page web de simulation d'hameçonnage, ce qui signifie que dans l'ensemble, 13,4 % (figure 2) des participants au tournoi ont fourni leur mot de passe.

Ces chiffres ont connu une hausse substantielle par rapport au Gone Phishing Tournament de 2019, où seulement 11 % des participants ont cliqué sur des liens de courriels d'hameçonnage, et un faible 2 % d'entre eux ont soumis leurs identifiants.

Ces constats soulèvent l'absolue nécessité d'établir, de maintenir et d'optimiser un programme de formation de sensibilisation à la sécurité efficace, appuyé par des simulations d'hameçonnage reflétant la vie réelle. Ces deux outils s'alimentent et se renforcent mutuellement, favorisant ainsi une expérience d'apprentissage beaucoup plus complète et une culture d'entreprise nettement plus cybersécuritaire.

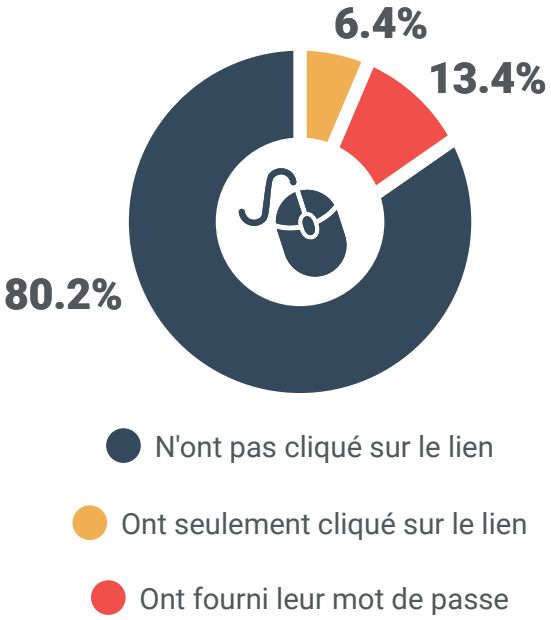
RÉPONSES AU SITE WEB D'HAMEÇONNAGE

Figure 1



RÉPONSES TOUS UTILISATEURS

Figure 2



Le nombre accru de travailleurs à distance et hybrides souligne aussi l'importance de comprendre, de repérer et d'éviter les menaces d'hameçonnage les plus récentes. L'importance de l'infrastructure technique diminue alors que l'utilisateur adopte un style de travail flexible. L'usage d'appareils personnels pour accéder à un document d'entreprise, à un espace nuagique d'entreposage de données, à un serveur ou à compte de courriel est devenu monnaie courante.

Terranova Security a pris l'engagement de fournir à toutes les organisations les connaissances nécessaires pour se préserver des menaces les plus récentes et complexes. Aussi, même les organisations qui n'ont jamais participé au Gone Phishing Tournament peuvent avoir accès gratuitement à notre simulation d'hameçonnage pour voir comment leur taux de clics se mesure à celui des pairs de leur industrie, de leur région ou de leur taille organisationnelle.

Comment les attaques d'hameçonnage affectent toutes les organisations

Un hameçonnage réussi peut immédiatement nuire financièrement à une entreprise, à ses investisseurs et à ses partenaires. Elle peut également affecter sérieusement sa rentabilité à long terme en altérant sa réputation. Ou encore, elle peut miner la confiance des citoyens envers leur gouvernement local ou leurs institutions de santé.

Des PME aux sociétés multinationales, aux universités, aux hôpitaux et agences gouvernementales, les attaques d'hameçonnage peuvent avoir des répercussions désastreuses sur une organisation.

Le travail à distance entraîne plusieurs enjeux de sécurité qui n'ont possiblement pas été totalement réglés par le passé. En travaillant à distance, le risque de fuite de données vers des individus non autorisés augmente. Les utilisateurs relâchent souvent leurs pratiques sécuritaires hors du bureau. Il faut également prendre en compte la rapidité avec laquelle les organisations ont eu à déployer leur personnel en télétravail et à communiquer aux utilisateurs à distance la série de risques pouvant les menacer durant leur travail à domicile.

L'hameçonnage continue de susciter une grande inquiétude comme principale forme d'attaque ciblant les utilisateurs. On peut facilement imaginer que pour les organisations, il était prioritaire de maintenir les opérations et la rentabilité tout en minimisant les perturbations et les coûts, et que celles-ci n'ont pas eu le temps ou l'argent requis pour éduquer convenablement un personnel à distance.

Plusieurs consommateurs, investisseurs, fournisseurs tiers et autres veulent éviter toute association avec des organisations ayant été victimes d'une attaque par hameçonnage. Dans un monde où les données revêtent plus de valeur que jamais, le défaut de protéger l'information confidentielle peut entacher de façon permanente l'image publique d'une organisation, surtout si elle n'a pas été capable de renforcer ses initiatives de sensibilisation à la sécurité.

Dans son rapport de 2019 intitulé Internet Crime Report, le Centre de plaintes envers les crimes par Internet du FBI (IC3) indique avoir reçu chaque jour près de 1 300 plaintes reliées à l'hameçonnage, ce qui a entraîné des pertes de milliards de dollars autant pour les personnes que pour les entreprises qui en ont été victimes. Selon l'IC3, la fraude du PDG (un type d'hameçonnage) à elle seule a coûté 26 G$ jusqu'ici.

Les impacts d'une attaque d'hameçonnage réussie ont une portée impressionnante, surtout lorsque les employés sont plus dispersés. La cybersécurité entourant l'accès, le partage, l'entreposage et la modification de tous les types de données se complexifie. Si à cela on ajoute l'utilisation d'appareils personnels, les cybercriminels disposent d'une quantité incroyable d'occasions à saisir.

L'importance des simulations d'hameçonnage

Les profonds changements causés par la pandémie du coronavirus ont transformé radicalement l'approche des organisations envers la cybersécurité. Avec un nombre accru de personnes travaillant hors de la sécurité numérique qu'offrent l'environnement de travail au bureau, le besoin de mettre l'accent sur le facteur humain dans la protection des données prend maintenant une importance inégalée.

Lorsque les organisations mettent la priorité sur les personnes dans leurs processus de sécurité de l'information, elles leur fournissent les connaissances, les outils, la confiance et le soutien nécessaires pour se protéger des dernières cybermenaces. Malheureusement, cette année, les résultats du tournoi indiquent des taux de clics et des partages d'identifiants qui dénotent un retard important dans les pratiques de plusieurs organisations à cet égard.

Même si les barrières techniques peuvent sembler hermétiques, il demeure que dans une organisation, c'est l'utilisateur qui constitue la principale ligne de défense contre les cybermenaces. Aussi, en exposant vos employés à des scénarios d'apprentissage reproduisant la réalité avec des simulations d'hameçonnage, leurs comportements sont mis à l'épreuve dans un environnement sécuritaire, et vous leur donnez l'autonomie dont ils ont besoin pour prendre les bonnes décisions lorsque survient une situation réelle.

En sachant qu'il suffit d'un faux pas pour ouvrir une ou plusieurs portes aux cybercriminels pour accéder à des informations sensibles personnelles ou d'entreprise, une vigilance constante est cruciale. Pour pouvoir repérer et éviter les menaces d'hameçonnage, la méfiance de l'utilisateur doit être alimentée et encouragée par des simulations d'hameçonnage dynamiques et actuelles face aux risques émergents.

Les simulations d'hameçonnage intégrées aux initiatives de formation de sensibilisation à la sécurité permettent aux organisations de :

1. Réduire considérablement le niveau de menaces et de risques;
2. Rehausser la sensibilisation de l'organisation à l'égard des fraudes émergentes;
3. Minimiser les coûts associés aux attaques d'hameçonnage qui réussissent;
4. Mesurer précisément les niveaux de vulnérabilité individuels et organisationnels;
5. Atténuer le réflexe de confiance spontanée en modifiant le comportement de l'utilisateur;
6. Fournir aux employés une rétroaction ciblée et une formation juste-à-temps au besoin;
7. Améliorer chez l'utilisateur le signalement et la réaction aux tentatives d'hameçonnage;
8. Appliquer une formation sur l'hameçonnage spécifique au rôle pour en rehausser la pertinence;
9. Protéger les données confidentielles, personnelles ou d'entreprise;
10. Instaurer une culture de cybersécurité alimentée par des cyber héros.

À eux seuls, les pare-feu, les mises à jour, les correctifs et les logiciels de sécurité ne constituent pas une protection suffisante dans un monde où les fraudes par hameçonnage font partie du quotidien. En omettant le facteur de risque humain dans l'équation, il est impossible d'en arriver à une culture prônant la cybersécurité.

La méthodologie du Gone Phishing Tournament

Chaque année, le tournoi est ouvert à tous les responsables de la sécurité. Les organisations participantes en 2020 comprenaient des clients actuels de Terranova Security autant que des intervenants n'ayant aucune relation antérieure avec nous en tant que leur fournisseur de sensibilisation en sécurité.

L'objectif de cet exercice mondial annuel de simulation d'hameçonnage est de mesurer et d'évaluer le taux de détection des employés envers des menaces d'hameçonnage réalistes qui pourraient survenir dans leur quotidien.

Toutefois, les résultats du Gone Phishing Tournament, contrairement à d'autres rapports annuels comparatifs en matière de formation de sensibilisation à la sécurité, présentent des données offrant une comparaison plus performante et précise entre tous les participants. Le tournoi était accessible à toutes les organisations sans égard à leur secteur d'activité, à leur taille ou à leur emplacement géographique, clientes ou non de Terranova Security.

Plutôt que d'évaluer la performance au moyen d'une grande variété de scénarios d'hameçonnage, chacun reproduisant un contexte variable, le Gone Phishing Tournament utilise la même simulation d'hameçonnage durant tout son déroulement.

C'est cette cohérence qui permet une comparaison rigoureuse et objective du taux de clics et de partages d'identifiants en ligne. Chaque utilisateur voit le même courriel et la même page web d'hameçonnage, durant le même laps de temps, et dans sa langue maternelle.

Cette partie du rapport donne de l'information détaillée sur la méthodologie du Gone Phishing Tournament de 2020, sur la simulation comme telle, ainsi qu'une vue d'ensemble des participants et de la stratégie mondiale de l'événement.

Au sujet du modèle de simulation

Cette année, les modèles de courriel et de page web ont été fournis par Microsoft. Ils reflétaient un scénario réaliste auquel tout utilisateur, surtout un travailleur à distance, pourrait être confronté. Le modèle de scénario a été choisi par l'équipe de direction de Terranova Security. Il visait à mesurer plusieurs comportements de l'utilisateur, notamment sa tendance à cliquer sur le lien d'un courriel douteux et à fournir des données – ici il s'agissait de ses identifiants de connexion – dans un formulaire sur une page web.

Le niveau de difficulté du modèle a été rehaussé par rapport à la simulation de l'année dernière. Les experts de Terranova Security ont estimé sa complexité de moyenne à haute, en fonction du nombre d'indices indiquant un hameçonnage et de la difficulté à repérer les divers signes signalant un danger. Le courriel et la page web ont été personnalisés en utilisant l'adresse courriel du destinataire, ils ne contenaient aucune faute d'orthographe et avaient un aspect authentique. Le scénario regroupait donc les tactiques que tout cybercriminel, sans trop d'efforts et de raffinements, peut appliquer dans ses activités d'hameçonnage.

Cette décision avait pour but de donner aux utilisateurs la vraie saveur des menaces d'hameçonnage en évolution perpétuelle qui touchent les professionnels de toutes les industries.

Pour maximiser l'accessibilité, la lisibilité et la réceptivité, le modèle du tournoi de 2020 supportait 12 langues, soit :

- Anglais
- Allemand (DE)
- Chinois simplifié (ZH-CN)
- Chinois traditionnel (ZH-HK)
- Coréen (KO)
- Espagnol Espagne (ES-ES)
- Français Canada (FR-CA)
- Français France (FR-FR)
- Italien (IT)
- Japonais (JA)
- Portugais Brésil (PT)
- Russe (RU)

Pour ajouter un piège dans l'édition 2020 du Gone Phishing Tournament, le premier courriel d'hameçonnage semblait provenir d'une source fiable et de l'adresse : noreply@easysharefolder.com.

De plus, l'objet du courriel était délibérément conçu pour correspondre à des échanges de courriels dans un contexte de travail à distance pour refléter la réalité actuelle. L'objet mentionnait « Une mise à jour de la politique sur le travail à distance a été partagée avec vous. »

Le courriel pressait les destinataires d'ouvrir un document contenant prétendument une mise à jour de la politique organisationnelle sur le travail à distance. Une fois cliqué, le lien les redirigeait vers une page d'accueil contrefaite selon l'image de marque de Microsoft, où on leur demandait d'entrer le mot de passe associé à leur compte de courriel professionnel.

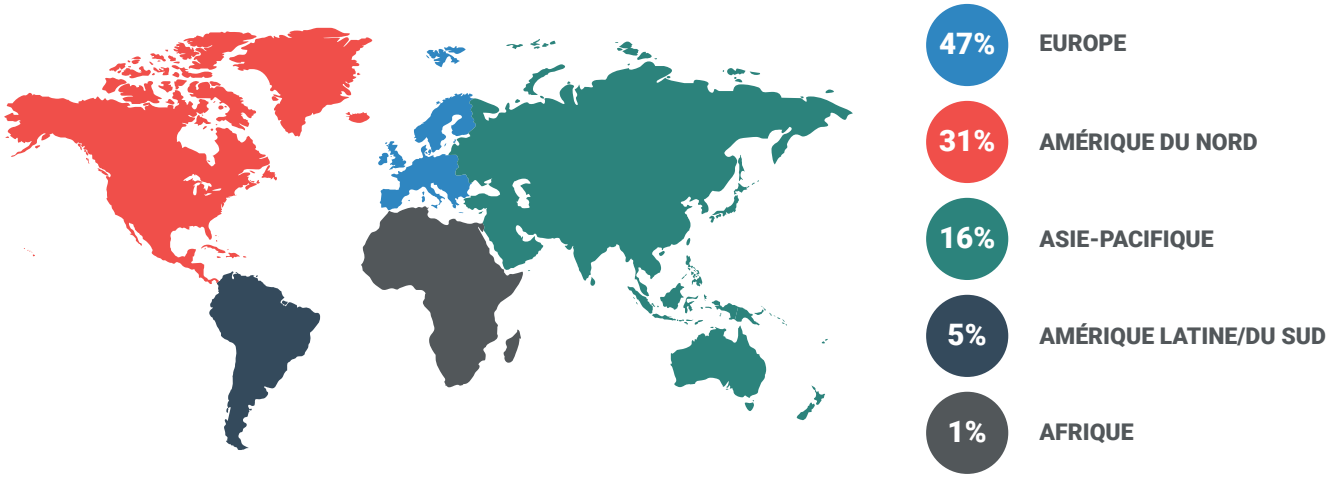
Au sujet des participants

En 2020, le Gone Phishing Tournament a accueilli 57 % plus d'organisations participantes qu'à l'édition de 2019, avec une augmentation des utilisateurs de 90 %.

Le tournoi a également joui d'un rayonnement mondial plus important puisque les utilisateurs de 98 pays différents ont participé à la simulation (figure 3).

RÉGIONS PARTICIPANTES

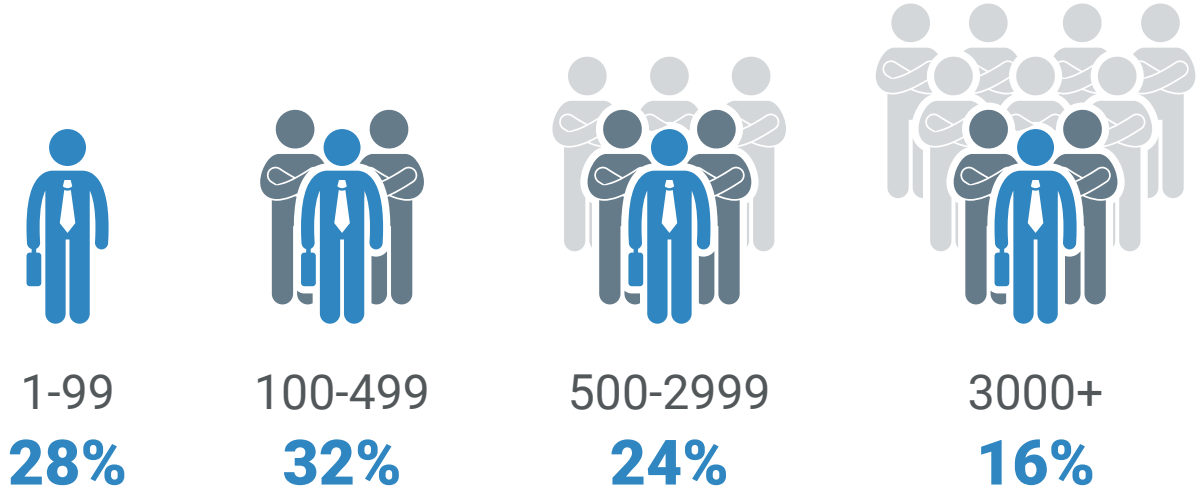
Figure 3



La taille et le secteur d'activité des organisations participantes étaient très variés. Une proportion de 28 % d'entre elles étaient des PME comptant moins de 100 employés. Les entreprises intermédiaires de 100 à 499 employés représentaient 32 %, et celles de 500 à 2 999 employés comptaient pour 24 %. Des organisations participantes, 16 % employaient 3 000 personnes ou plus (figure 4).

TAILLE DES ORGANISATIONS

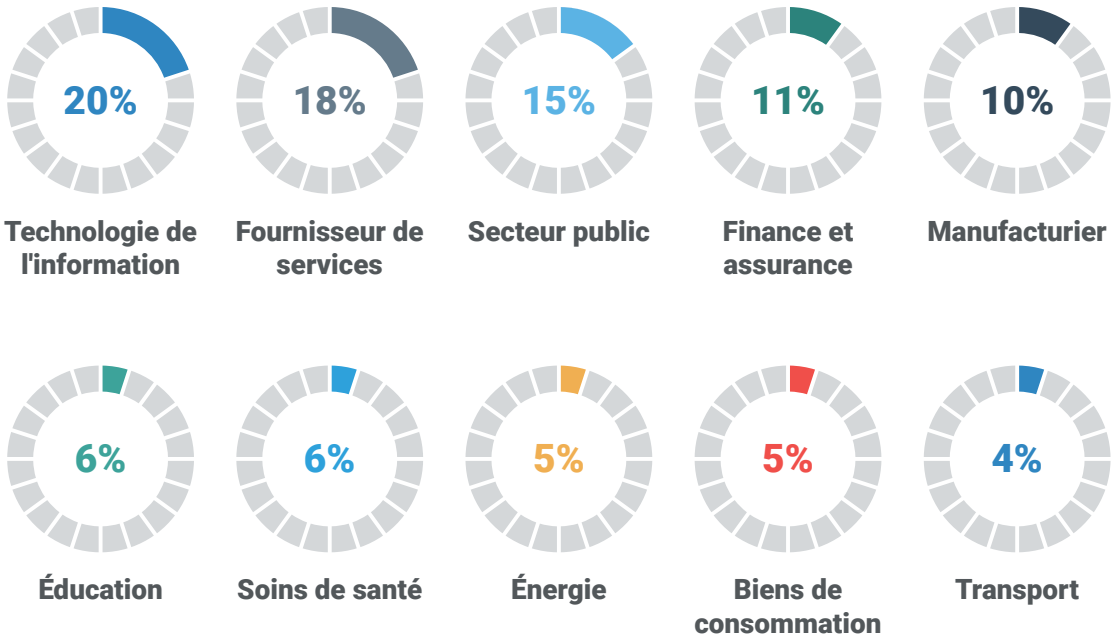
Figure 4



Les organisations qui ont complété le tournoi de 2020 provenaient de ces secteurs (figure 5) :

SECTEURS PARTICIPANTS

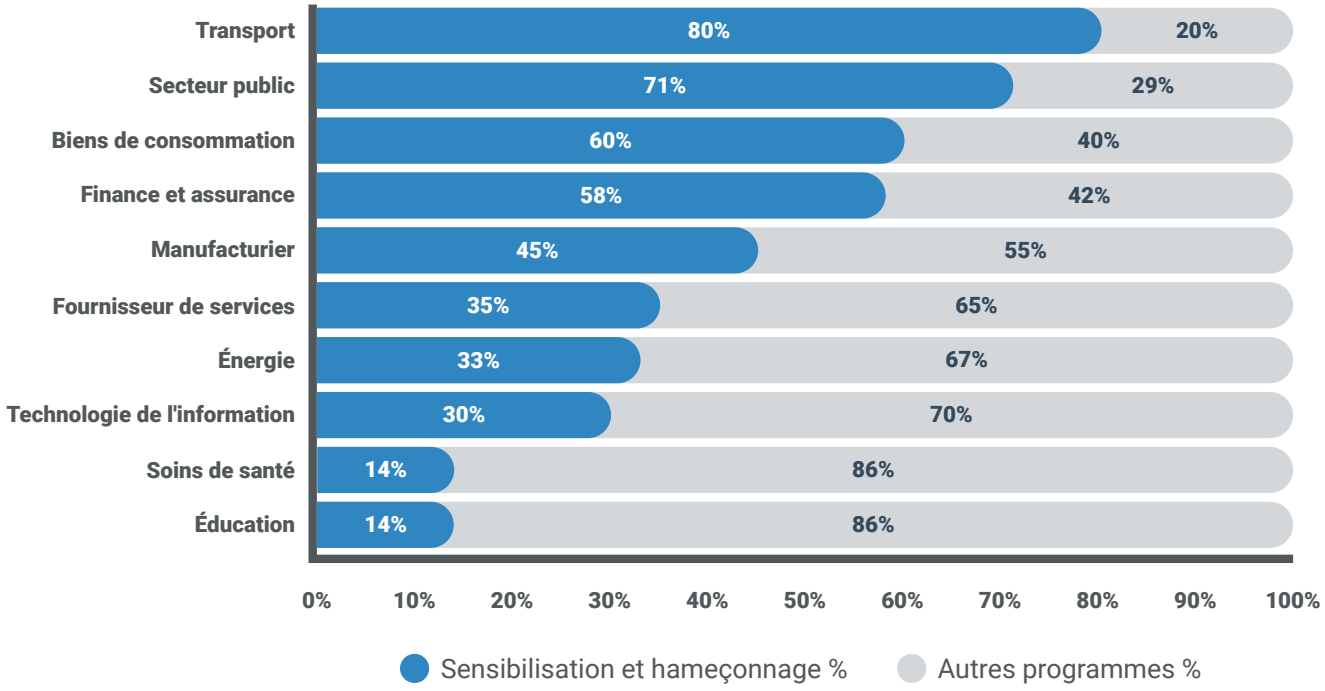
Figure 5



La nature du programme de sensibilisation à la sécurité existant dans chacune des organisations participantes variait considérablement, selon le secteur. Par exemple, 80 % de celles en transport avaient déjà en place un programme de formation englobant des modules éducationnels sur la sensibilisation à la sécurité et des simulations d'hameçonnage, ce qui constitue une combinaison idéale (figure 6).

TYPE DE PROGRAMME PAR SECTEUR

Figure 6

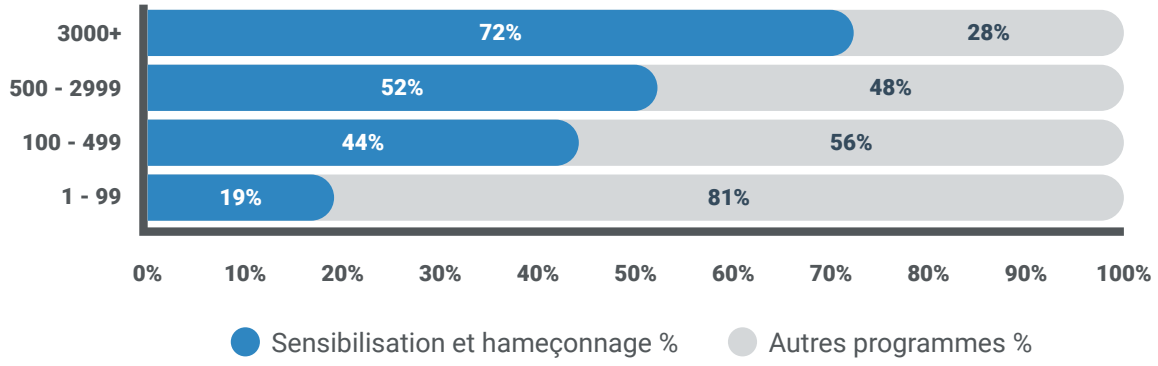


À l'inverse, des secteurs comme l'éducation et les soins de santé accusaient un retard important puisque seulement 14 % dans ces catégories avaient déployé ces ceux types d'initiatives. Fait étonnant, seulement 30 % des organisations en technologie de l'information offraient à leurs utilisateurs cette combinaison idéale.

Les programmes de formation existants sont devenus plus robustes et dynamiques à mesure que le nombre d'employés grimpait. Seulement 19 % des PME ont indiqué que leur programme intégrait des modules éducationnels de sensibilisation à la sécurité et des simulations d'hameçonnage, comparativement à 72 % de celles de moins de 3 000 employés (figure 7).

TYPE DE PROGRAMME PAR TAILLE

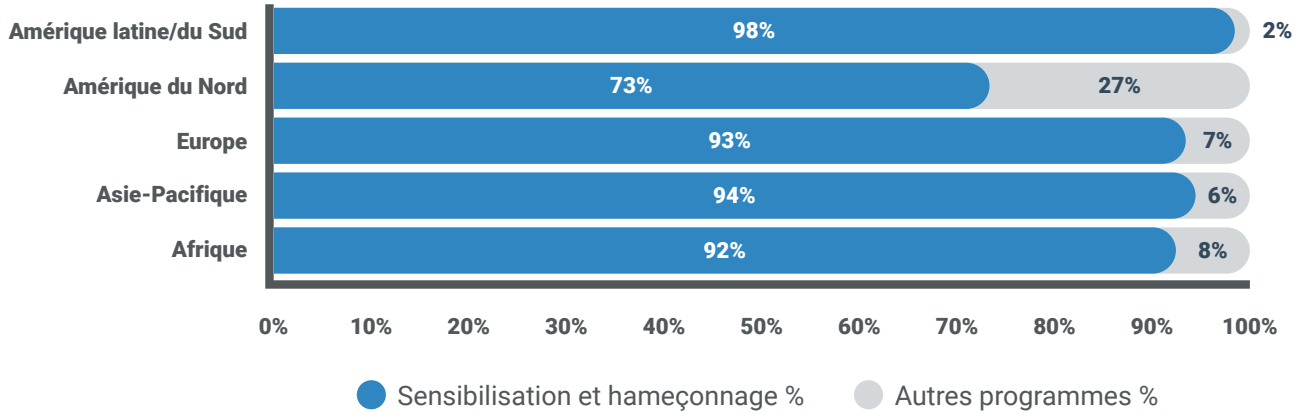
Figure 7



Les utilisateurs des organisations de l'Amérique du Nord ont été exposés à des activités de sensibilisation et de simulation d'hameçonnage dans une proportion de 73 %, un taux plus bas que les organisations du reste du monde (figure 8).

EXPOSITION DES UTILISATEUR AUX ACTIVITÉS DE SENSIBILISATION

Figure 8



Au sujet de la stratégie

La deuxième édition du Gone Phishing Tournament se déroulait sur 11 jours consécutifs, en octobre 2020. Durant tout le processus, Terranova Security a appliqué les mêmes contrôles de sécurité habituels sur les données de sa plateforme de sensibilisation à la sécurité. Cette particularité signifie que durant le tournoi, aucune donnée entourant les mots de passe fournis par les utilisateurs à l'aide des formulaires web n'a été recueillie, et que le niveau de sécurité de l'information le plus élevé a été respecté tout au long de l'événement.

Lorsque les utilisateurs entraient leurs informations de connexion, ils étaient immédiatement dirigés vers une page de commentaires à propos de la simulation d'hameçonnage qui soulignait les signes de fraude qu'ils n'avaient pas détectés. La page mettait également en valeur plusieurs pratiques essentielles à observer en tout temps lors d'une attaque d'hameçonnage de ce type.

À la fin de la simulation, Terranova Security a amorcé l'étape de l'analyse de données. Toute l'information fournie par les participants a été anonymisée et, au terme de l'analyse, les données utilisées durant le processus ont été supprimées pour assurer une confidentialité et une sécurité totales aux utilisateurs participants.

Somme toute, le succès remporté par le Gone Phishing Tournament est lié à l'habileté d'une organisation à comparer ses taux de clics à d'autres dont les caractéristiques sont similaires. Ainsi, une PME du secteur de la technologie de l'information a besoin de données lui fournissant un portrait réel de sa performance par rapport à celle de ses pairs, soit de même envergure ou du même secteur, pour répondre à la question qui est au cœur de l'événement : Comment mon taux de clics se compare-t-il?

Ce principe sous-jacent, combiné au fait que chaque utilisateur est testé selon la même simulation d'hameçonnage, signifie que l'organisation obtient une compréhension plus profonde et exacte de sa situation à l'égard de la protection de ses données contre les cybercriminels.

Les résultats du Gone Phishing Tournament

Les attaques d'hameçonnage exploitent la tendance fondamentalement humaine de faire confiance aux autres qui, règle générale, pousse l'utilisateur à cliquer sur des liens qui apparaissent dans un courriel ou un SMS. Pourtant, comme le démontre ce rapport, même les liens d'hameçonnage à l'apparence inoffensive peuvent constituer des portes d'entrée pour les activités criminelles.

Cliquer sur un lien d'hameçonnage n'est que le début. Alimentée par l'intelligence en temps réel de Microsoft, la simulation conçue pour ce tournoi a tenté d'attirer les utilisateurs vers une page web d'hameçonnage leur demandant d'entrer leur mot de passe. Une fois cette information obtenue, les cybercriminels s'empresseront sans doute de l'utiliser pour accéder à des données confidentielles et commettre des actes frauduleux au nom de la victime et à son insu.

Le niveau de difficulté accru du modèle de cette année, combiné au facteur de confiance humaine, a mené à un taux de clics plus élevé que lors du tournoi de 2019. Puisqu'un modèle unique a été appliqué à tous les participants, cette combinaison de tactiques a eu un effet universel sur l'ensemble des utilisateurs, soit de les inciter à compromettre leurs données.

Le rapport d'analyse comparative sur l'hameçonnage de 2020 examine l'ensemble des résultats et des tendances avant de décortiquer les données de l'événement par industrie, par taille de l'organisation et par région.

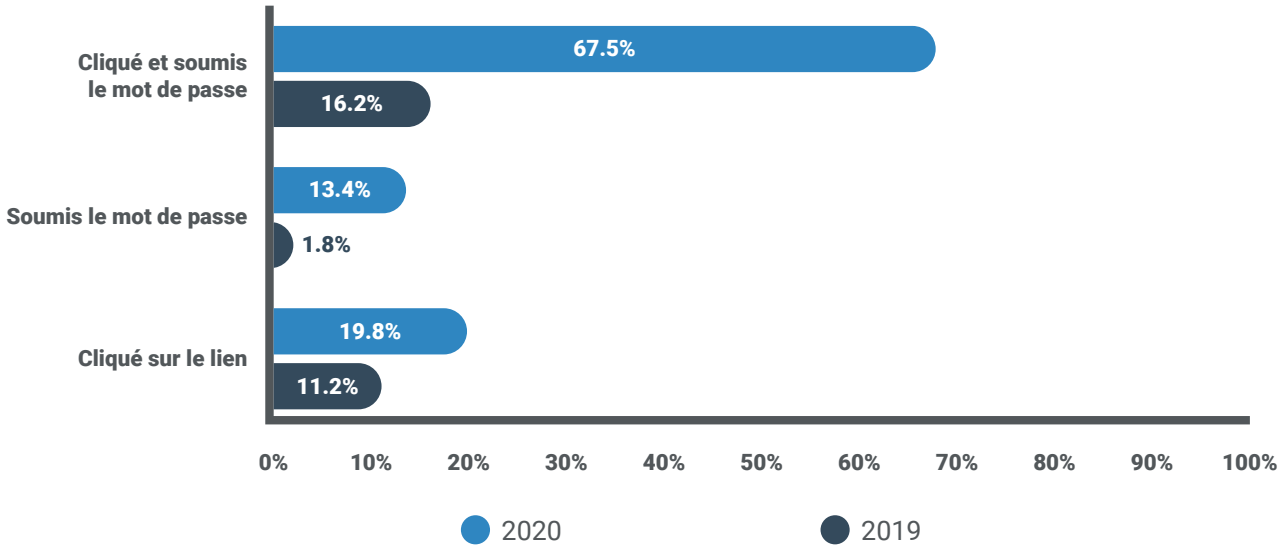
Vue d'ensemble des résultats

Comparativement au Gone Phishing Tournament de 2019, les utilisateurs ayant participé à l'édition de 2020 étaient plus enclins à cliquer sur le lien du courriel de la simulation d'hameçonnage. En conséquence, ceux qui ont fourni leurs identifiants de connexion sur la page web d'hameçonnage ont été considérablement plus nombreux.

Parmi tous les utilisateurs ayant participé au tournoi de 2020, 19,8 % ont cliqué sur le lien du courriel d'hameçonnage, une hausse de près de 9 points de pourcentage par rapport au tournoi de 2019. Les utilisateurs ont aussi entré de l'information sensible sur le formulaire web à 13,4 %, plus de 11 points de pourcentage de plus que l'an dernier (figure 9).

COMPARAISON ENTRE 2019 ET 2020

Figure 9



Quoi qu'il en soit, la tendance probablement la plus inquiétante a été le nombre de cliqueurs qui ont fini par remplir le formulaire web, soit un effarant 67,5 %. Comme le rapport l'indique précédemment, les experts de la sensibilisation à la sécurité de Terranova Security mentionnent qu'un taux moyen de 50 % de personnes qui cliquent et remplissent le formulaire est plus typique durant les simulations d'hameçonnage.

Pour placer les choses en contexte, considérons l'impact de ces chiffres sur une organisation de 1 000 employés. Sur la base de ces résultats d'ensemble, si cette simulation d'hameçonnage avait été une véritable attaque, près de 200 employés auraient cliqué sur le lien malveillant, et 134 d'entre eux auraient compromis leur information de connexion, le tout durant un seul incident d'hameçonnage.

Répartition des données par industrie : quels secteurs s'en sont le mieux tirés?

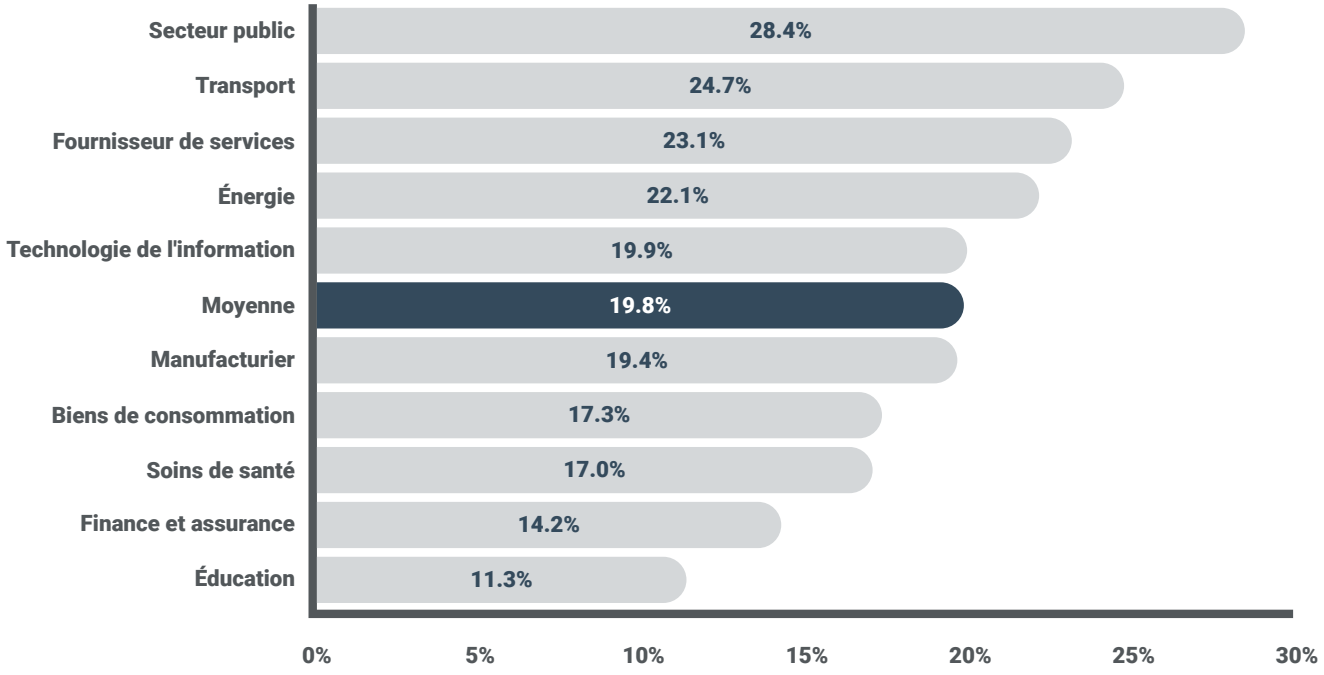
L'analyse des résultats du Gone Phishing Tournament de 2020 a démontré la variété des enjeux qui affectent les organisations, de diverses façons. Parce que tous les secteurs sont différents et qu'ils ne fonctionnent pas selon les mêmes normes de sécurité de l'information, une organisation doit comparer son taux de clics et de soumission d'identifiants à des joueurs similaires.

Comme l'illustrent les graphiques suivants, cinq industries ont enregistré des taux de clics sur des liens d'hameçonnage dépassant la normale (figure 10) :

- Le secteur public
- Le transport
- Les fournisseurs de services
- L'énergie
- La technologie de l'information

CLICS SUR LE LIEN PAR INDUSTRIE (%)

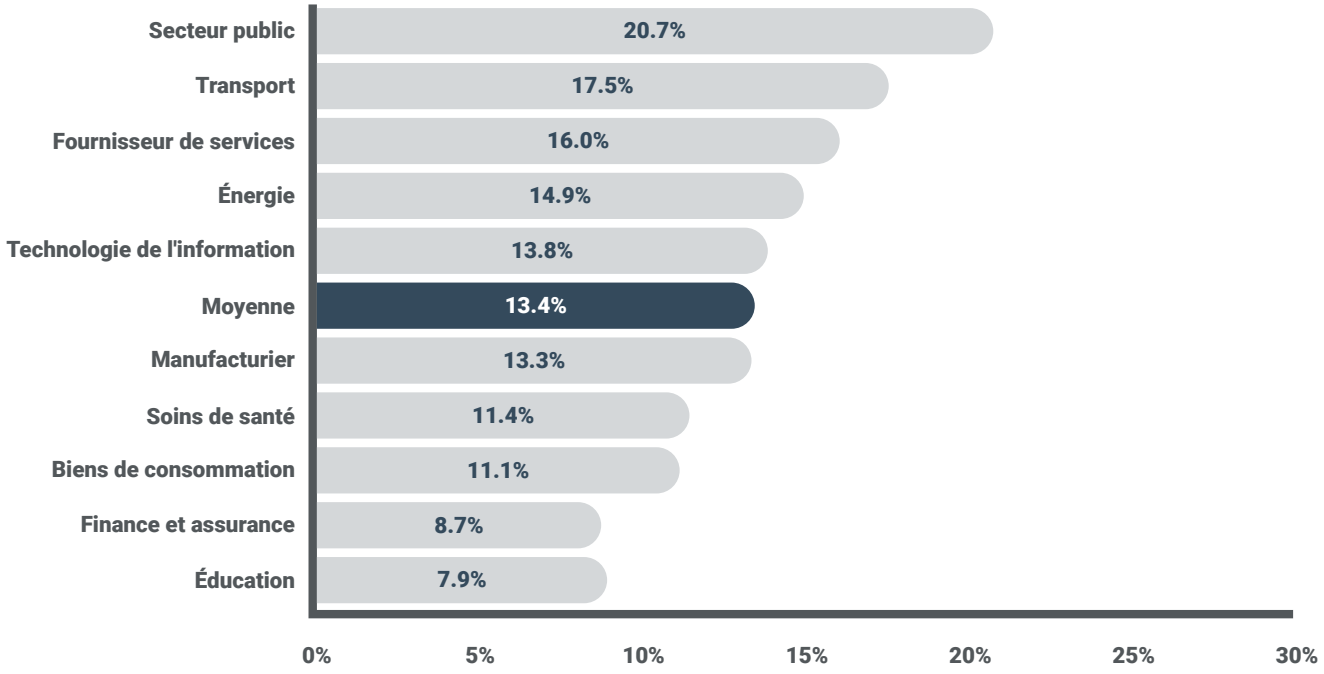
Figure 10



Ces cinq industries ont aussi enregistré un taux d'entrée de données sur formulaire web plus élevé que la moyenne du tournoi (figure 11).

PARTAGE DU MOT DE PASSE PAR INDUSTRIE (%)

Figure 11



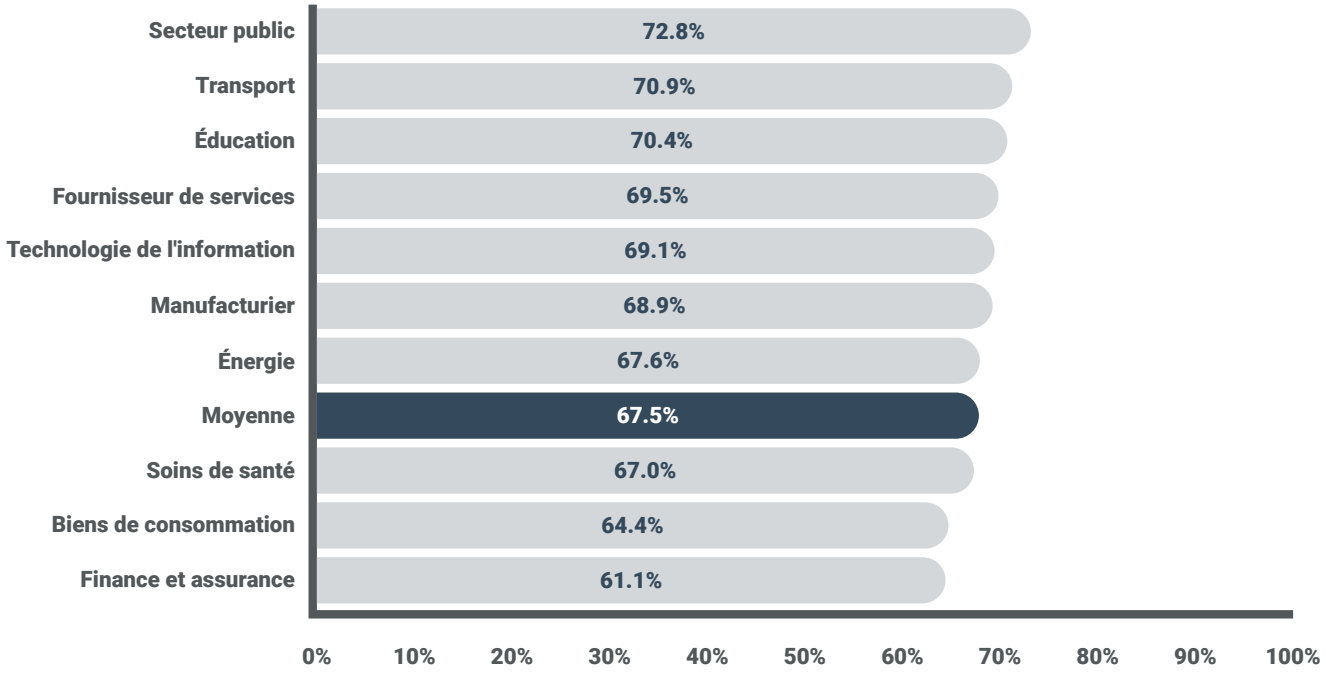
Par ailleurs, seulement deux industries ont enregistré un taux de clics inférieur à 15 % : la finance et l'assurance, et l'éducation. Ces mêmes deux secteurs ont également mieux performé que d'autres en ce qui concerne la soumission d'identifiants, en se classant bien au-dessus de la moyenne du tournoi, à 8,7 % et 7,9 % respectivement.

Les données précisant dans quelles industries on retrouve le plus grand nombre de cliqueurs ayant également compromis leurs identifiants de connexion constituent un échantillonnage fascinant quant à la formation moderne de sensibilisation à la sécurité.

Trois catégories de l'industrie, soit le secteur public, le transport, et l'éducation, enregistrent toutes des taux de clics et de soumission de données dépassant les 70 % (figure 13). En gros, cette variation signifie qu'au moins 7 utilisateurs sur 10 ayant cliqué sur le lien du courriel d'hameçonnage ont aussi compromis des données sensibles. Les fournisseurs de services, la technologie de l'information, et le secteur manufacturier n'étaient pas très loin derrière, avec un taux de clics et soumission de données de 68,9 % ou plus.

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

Figure 12



Quant aux meilleurs dans cette catégorie, le secteur de la finance et de l'assurance a obtenu le taux le plus bas à 61,1 %, suivi de près par celui des biens de consommation, à 64,4 %. Il demeure toutefois que ces taux représentent une tendance au clic et soumission chez au moins 6 personnes sur 10, un chiffre qui n'impressionnera probablement aucun chef d'entreprise ou expert en cybersécurité.

La répartition des résultats par industrie dénote le besoin incontestable d'intégrer à tout programme de sensibilisation à la sécurité des simulations d'hameçonnage, qui sont actualisées pour refléter les dernières menaces. En cette ère d'accélération de la transformation numérique et de dispersion de l'effectif, les employés doivent pouvoir identifier les attaques complexes potentielles et s'en protéger. Le scénario d'attaque de Microsoft en est un bon exemple puisqu'il reflète la réalité d'un vrai courriel d'hameçonnage.

En n'agissant pas, d'énormes quantités de données risquent d'être exposées, ce qui affectera la rentabilité des industries participantes et plus.

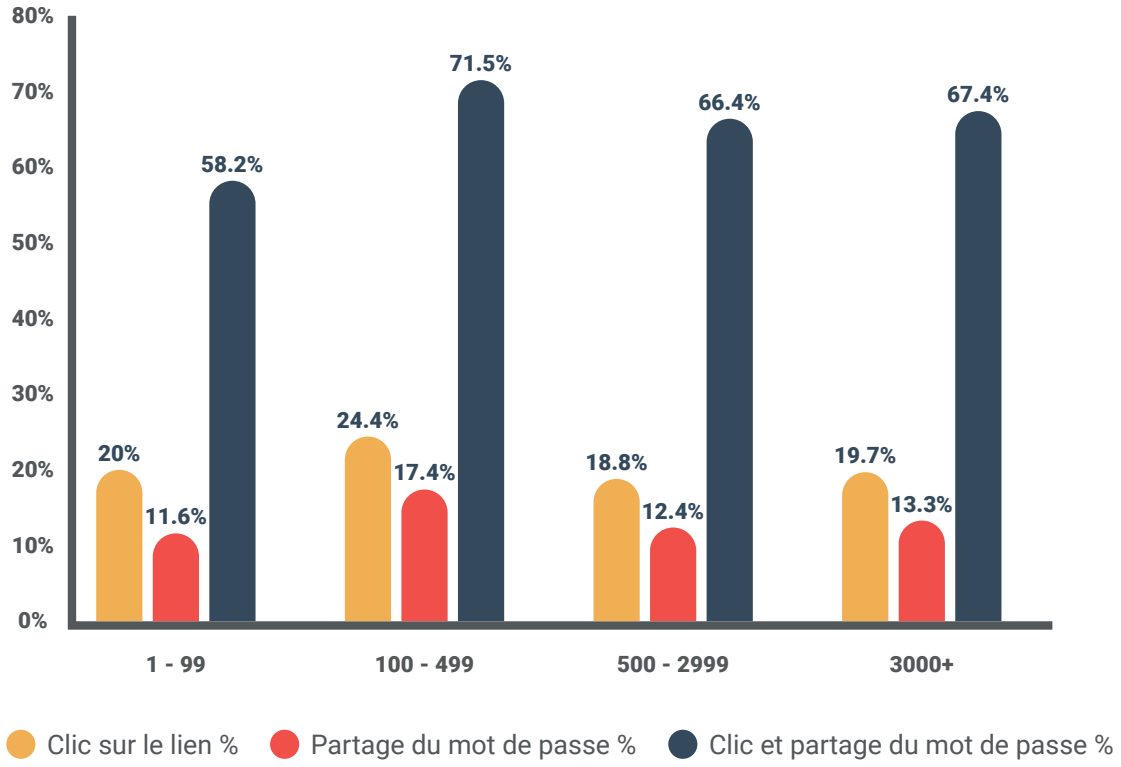
Répartition des données selon le nombre d'employés : la taille de l'organisation influence-t-elle les résultats?

Le Gone Phishing Tournament de 2020 a fait surgir l'éternelle question : les plus gros sont-ils les meilleurs? En d'autres mots, est-ce que la taille d'une organisation (et possiblement les ressources dont elle dispose) influence le facteur humain dans son infrastructure de protection des données?

Si l'on en croit les résultats de ce tournoi, la réponse est non (figure 13), puisque la simulation d'hameçonnage a eu un impact semblable pour les organisations, toutes tailles confondues.

RÉSULTATS PAR TAILLE D'ORGANISATION (%)

Figure 13



Comme le démontre le graphique, les PME se débrouillent mieux dans toutes les industries. Cette catégorie a obtenu un taux de clics de 20 % (au 2e rang), de 11,6 % en soumission de données, et de 58,2 % de clic et soumission. Sans être spectaculaires, ces résultats sont plus encourageants que ceux des organisations plus importantes.

Dans les trois dernières catégories de tailles, les organisations de 500 à 2 999 employés ont le mieux performé, avec le meilleur taux de clics à 18,8 %, et un taux de soumission de données à 12,4 %. Cependant, avec un rapport clic/soumission dépassant 66 %, le taux de soumission de données aurait été beaucoup plus dommageable si l'attaque avait été réelle et non simulée.

La répartition des résultats par le nombre d'employés soulève l'importance de mettre en place un programme de sensibilisation à la sécurité soutenu par des simulations d'hameçonnage réalistes. Quelle que soit sa taille, une organisation subira des conséquences relativement sévères si un nombre important de ses employés compromettent leur mot de passe.

Bien que Terranova Security ne puisse connaître la réalité spécifique à chaque organisation participante, il demeure que certaines inférences logiques se dégagent nettement :

- Les organisations de taille plus modestes n'ont pas toujours un service de TI dédié ou des ressources internes consacrant temps et énergie à planifier et mettre en œuvre un programme complet de sensibilisation à la sécurité avec simulations d'hameçonnage.
- Les organisations de grande taille, alors qu'elles sont probablement mieux positionnées en termes de personnel et de ressources, ont toutefois de la difficulté à communiquer dans toutes les unités de l'entreprise afin d'obtenir une adhésion générale au programme de formation.
- La montée en popularité du télétravail implique inévitablement une plus grande interaction des employés avec les fournisseurs et partenaires. Cette réalité rend encore plus criant le besoin de formation sur l'hameçonnage en raison du nombre de facteurs qui sont hors du contrôle de l'organisation.

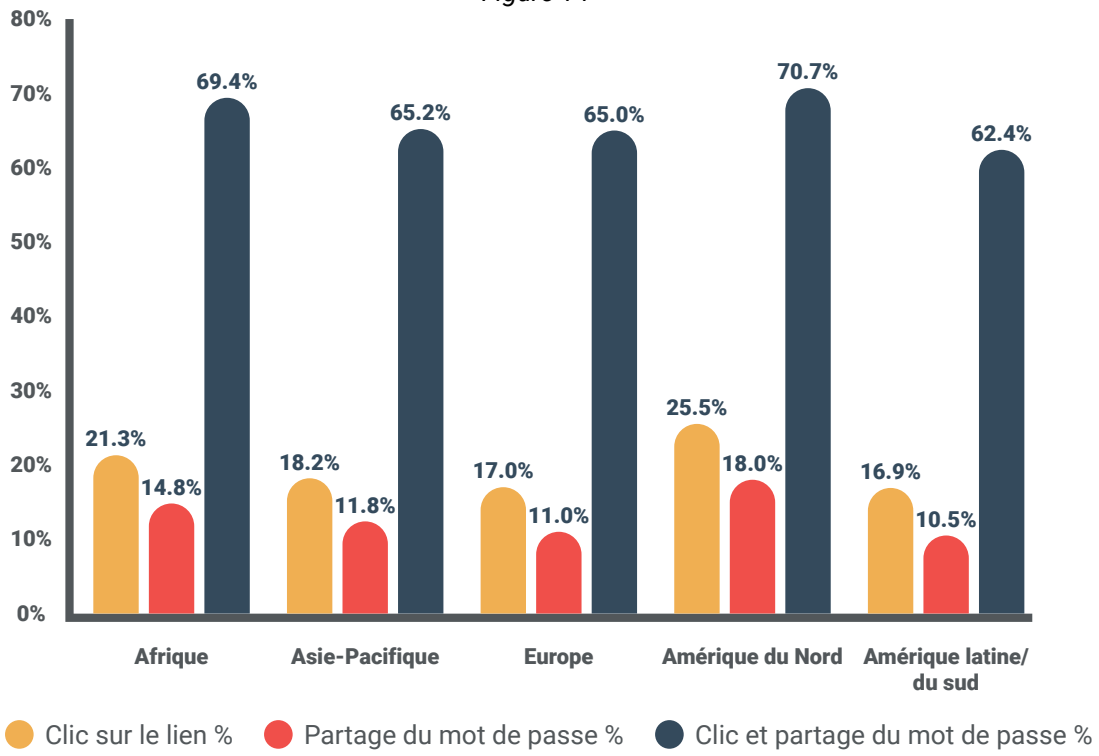
Répartition des données par région: la localisation d'un utilisateur est-elle importante?

L'augmentation du travail à distance ou de la main-d'œuvre hybride a considérablement affecté l'infrastructure de cybersécurité des organisations. Les employés et leurs appareils professionnels n'étant plus enchaînés à un environnement de bureau, ces organisations et leur personnel informatique ne peuvent pas compter uniquement sur les logiciels et les VPN pour protéger leurs données confidentielles.

Cette nouvelle réalité n'a fait que rendre plus urgent le besoin d'une formation sur l'hameçonnage universelle et à jour, dès 2021 et pour les années à venir. La nature urgente de ce manque de connaissances est reflétée en détail dans les résultats relatifs aux régions inclus dans ce rapport (figure 14).

RÉSULTATS PAR RÉGION (%)

Figure 14



L'Amérique du Nord a terminé à la dernière place sur cinq les régions participantes. Plus d'un quart des utilisateurs participants de cette région ont cliqué sur le lien du courriel d'hameçonnage et près de 20% ont soumis leur identifiant via le formulaire Web. Ces résultats se traduisent par environ 7 cliqueurs sur 10 ayant exposé des données de connexion sensibles.

À l'inverse, les utilisateurs basés en Europe ont affiché de meilleurs résultats, avec un taux de clic de 17% et une soumission d'identifiant à un taux de 11%. Les utilisateurs basés en Amérique du Sud et en Amérique latine ont affiché les meilleurs résultats dans l'ensemble, avec des taux respectifs de 16,9% et 10,5%.

Les taux élevés de clic et de soumission d'identifiant générés par la simulation d'hameçonnage conçue par Terranova Security en collaboration avec Microsoft, peuvent être attribués à la nature très plausible et actuelle du titre du contenu autant qu'à sa complexité. Faisant appel directement aux politiques de travail à distance, le scénario a profité de l'anxiété et du haut sens des responsabilités que de nombreux professionnels peuvent ressentir lors de la transformation numérique de leur organisation.

Les menaces d'hameçonnage évoluent constamment vers de nouvelles façons d'inciter ou de pousser les utilisateurs à agir, que ce soit en cliquant sur un lien ou en téléchargeant un fichier malveillant. En tant que leader mondial dans le milieu des affaires et le secteur des technologies de l'information, les organisations nord-américaines doivent, en particulier, améliorer ces résultats si elles espèrent éviter les répercussions des cyberattaques qui se présentent.

Pour protéger, avec succès, leurs données contre les cybercriminels, les organisations doivent également optimiser leurs efforts de sensibilisation à la sécurité et y inclure des exemples sur les plus récentes fraudes dont les pirates peuvent s'inspirer. Si ces mesures ne sont pas prises au sérieux, cela peut avoir un impact sur leur réputation auprès des consommateurs quant au traitement, à la confidentialité et à la sécurité des données.

Comment faire de la simulation d'hameçonnage une priorité de la sensibilisation à la sécurité

Les simulations d'hameçonnage ajoutent une dimension supplémentaire à un programme de sensibilisation à la sécurité. Des simulations d'hameçonnage informatives, interactives et réelles (ainsi que du contenu de formation juste-à-temps) peuvent éduquer les utilisateurs rapidement et efficacement sur les tactiques employées par de véritables attaques d'hameçonnage.

En offrant des opportunités d'apprentissage diversifiées et inclusives à ses employés, toute organisation peut instantanément renforcer ses processus de protection des données. Ce que les outils de cybersécurité purement techniques, comme les logiciels antivirus ou d'autres applications de chiffrement, ne peuvent pas faire.

L'importance des campagnes de formation ciblées et basées sur les risques

Lors de la conception d'un programme de sensibilisation à la sécurité, il est essentiel d'établir un cadre qui crée un parcours d'apprentissage défini et efficace pour l'utilisateur. Pour y parvenir, Terranova Security a identifié les sept comportements liés aux risques que chaque organisation doit affronter pour renforcer la protection des données:

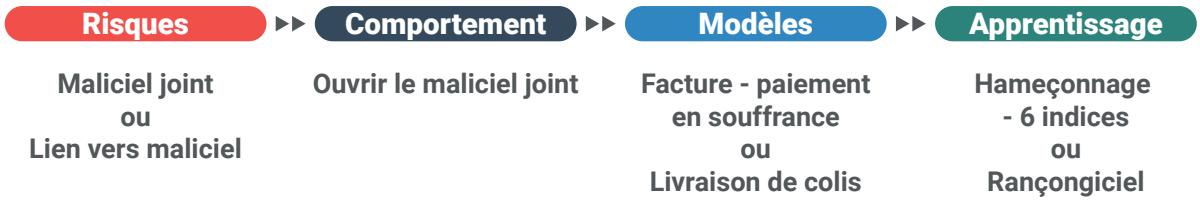
RISQUES

- Maliciel joint
- Lien vers maliciel
- Lien joint
- URL téléchargement furtif
- Autorisation d'applications
- Collecte d'identifiants
- Compromission courriel d'entreprise

COMPORTEMENTS

- Ouvrir le maliciel joint
- Cliquer sur le lien ou le bouton
- Fournir identifiant unique/mot passe
- Fournir info personnelle de l'employé
- Fournir info entreprise ou financière
- Fournir info personnelle identifiable
- Fournir info personnelle / financière

Exemple de formation selon le risque



Cette illustration démontre la connexion entre la menace, qui, dans ce cas, est un maliciel sous forme d'une pièce jointe ou d'un lien, et le comportement de l'utilisateur qui peut compromettre les données. Selon le type de comportement que vous souhaitez adresser, vous devez choisir des modules d'apprentissage et des simulations d'hameçonnage réelles qui reflètent ces risques et vous permettent de mesurer avec précision les changements de comportement.

Lors du lancement d'une campagne de sensibilisation à la sécurité, Terranova Security recommande d'utiliser des outils de communication pour encourager la participation dans toutes les unités d'affaires. Ensuite, commencez par un module d'introduction à l'hameçonnage afin d'établir les connaissances de base au sein de l'organisation.

Ceci est suivi d'un module de microapprentissage mensuel qui informe les utilisateurs sur un risque spécifique lié au comportement ciblé. La prochaine étape est une simulation d'hameçonnage directement liée sujet du microapprentissage.

Pour obtenir des informations tangibles sur le progrès des utilisateurs, les organisations effectuent en moyenne 4 à 6 simulations par années, avec au moins quatre activités de sensibilisation sur les menaces liées à l'hameçonnage. Terranova Security recommande de cibler une amélioration du taux de clics global de 5% à la suite de 4 à 6 simulations et activités de sensibilisation en continu sur une période de 12 mois.
Puisque les scénarios varient en termes de complexité et d'histoire, la probabilité que quelqu'un clique varie également.

Votre taux de clics moyen correspond au taux moyen de toutes les simulations effectuées au cours d'une période donnée, pas seulement la dernière. Par conséquent, il est impératif de former les utilisateurs à la détection d'une attaque par hameçonnage dès la première étape: le courriel d'hameçonnage.

7 étapes faciles pour une puissante formation en sensibilisation à l'hameçonnage

Adopter une approche proactive et basée sur les données pour la sensibilisation à la sécurité en utilisant des simulations d'hameçonnage du monde réel ne devrait pas être ardu. Pour éduquer les utilisateurs et changer les comportements qui pourraient mener à la compromission des données, suivez ces directives simples:

1. **Ciblez les bons comportements** des utilisateurs en explorant les données de cybersécurité existantes et en identifiant les actions spécifiques qui ont conduit à des violations de données.
2. **Créez des simulations d'hameçonnage** qui corrigent ces faiblesses et tirez parti de scénarios actuels que les utilisateurs peuvent rencontrer dans leur vie quotidienne.
3. **Collectez des données** de simulation d'hameçonnage en temps réel pour faciliter l'évaluation, la maintenance et le raffinement de vos initiatives de sensibilisation à la sécurité.
4. **Suivez et surveillez les progrès** des utilisateurs pour déterminer leur niveau de connaissance 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 modèles de simulation personnalisables** qui permettent à votre organisation d'adapter chaque aspect du processus de formation pour vous aider à atteindre vos objectifs spécifiques.
7. **Choisissez une solution évolutive et inclusive** qui propose une formation multilingue, accessible et un contenu adapté aux mobiles qui facilite l'éducation d'une base d'utilisateurs mondiale diversifiée.

Usez de transparence et améliorez le niveau de sensibilisation des employés face à l'hameçonnage

Même avec le programme de sensibilisation à la sécurité le plus dynamique, votre organisation peut encore être victime d'une attaque d'hameçonnage réussie. Si un incident survient, vos employés ont besoin d'une communication transparente et de l'assurance que les politiques appropriées et les prochaines étapes sont en place pour empêcher une attaque future.

Pour améliorer la sensibilisation des employés à l'hameçonnage grâce à ces pratiques, vous devez:

- Expliquez comment l'hameçonnage s'est produit, y compris les signaux d'alerte qui permettent d'identifier le courriel comme étant de l'hameçonnage ou une autre cybermenace.
- Utilisez des outils de communication tels que des vidéos, des infographies, des infolettres, et d'autres contenus partageables pour augmenter la sensibilisation et encourager la participation aux initiatives de formation.
- Créez un groupe interne de cyber héros ambassadeurs afin de soutenir les employés lorsqu'ils se méfient d'un message ou demande de téléchargement inattendu.
- Informez les employés sur l'omniprésence de l'hameçonnage grâce à des outils de communication et d'apprentissage diversifiés et interactifs.
- Insistez sur l'importance de la transparence des employés lors d'une attaque d'hameçonnage réussie, y compris comment la communication immédiate avec leur (s) gestionnaire (s) ou le département informatique, conformément à la politique existante de l'organisation, peut aider leur équipe à récupérer rapidement.

Prochaines étapes pour assurer le succès de la sensibilisation à la sécurité

Avec le travail à distance et la transformation numérique accélérée qui changent le paysage d'affaires tel que nous le connaissons, la sensibilisation à la sécurité et les simulations d'hameçonnage doivent être une réelle priorité pour toutes les organisations.

L'organisation d'un unique déjeuner-causerie sur les menaces de l'hameçonnage ou les formations en cybersécurité sporadiques ne sont plus utiles. Les cybercriminels modifient trop souvent leurs stratagèmes pour croire que des initiatives de formation peu fréquentes peuvent encore protéger les données.

Les organisations soucieuses de renforcer leurs défenses contre l'hameçonnage doivent donner la priorité à l'éducation des employés en leur donnant un accès cohérent à un contenu de sensibilisation à la sécurité de haute qualité et à des simulations hameçonnage engageantes, informatives et amusantes.

Les organisations doivent également reconnaître leurs points faibles et profiter des outils de communication comme des vidéos, des infographies, des infolettres par courriel et d'autres campagnes personnalisables pour améliorer leurs efforts de sensibilisation à la sécurité et renforcer l'adhésion de toutes les divisions ou départements.

Terranova Security recommande aux organisations d'utiliser toutes les opportunités possibles afin de collecter des données sur le niveau de sensibilisation des employés, les taux de clics et les normes de l'industrie. Avoir ces informations en main leur permettra de prendre des mesures proactives et créer un réel changement de comportement qui met fin à la confiance, le clic et la réponse automatique à la suite d'une menace par hameçonnage.

Par-dessus tout, il est essentiel que toute initiative de sensibilisation à la sécurité et à l'hameçonnage évolue continuellement pour inclure du matériel d'apprentissage inspiré des plus récentes menaces d'hameçonnage. Ce n'est qu'à ce moment-là que les employés d'une organisation pourront détecter et se protéger contre les attaques d'hameçonnage avec cohérence et confiance.

Votre partenaire de choix pour la sensibilisation à la sécurité

Terranova Security offre toujours aux leaders de la cybersécurité et aux utilisateurs de nouveaux contenus d'apprentissage pour les aider à acquérir de nouvelles connaissances sur des sujets clés relatifs à la sécurité de l'information. Si vous recherchez le bon endroit pour commencer votre parcours de sensibilisation à la sécurité, ne cherchez pas plus loin que le Hub de Cybersécurité!

Ce portail de contenu gratuit donne à toutes les organisations intéressées un accès amusant, engageant ainsi que des ressources faciles à partager telles que des infographies, des bandes dessinées, des vidéos, des guides détaillés et bien plus encore. De plus, les experts de Terranova Security mettent continuellement à jour le Hub afin que vous puissiez régulièrement consulter de nouveaux contenus.

Consultez-le dès maintenant!

Le Hub de Cybersécurité

Inscrivez-vous maintenant pour accéder à du contenu de sensibilisation à la cybersécurité engageant, facile à partager et disponible en plusieurs formats.

ACCÉDER AU HUB

Pour plus d'informations sur la solution de formation Terranova Security et comment elle contribue à l'autonomisation des dizaines de millions d'utilisateurs dans le monde grâce à un contenu de haute qualité et des simulations d'hameçonnage robustes, visitez TerranovaSecurity.com/fr.

Au sujet de Terranova Security

Fondée en 2001, Terranova Security est issue de la passion de sa fondatrice et CEO, Lise Lapointe, envers l'éducation, la formation et la technologie. Cette passion rejoint un besoin grandissant pour la sensibilisation à la cybersécurité et la formation, pour aider les organisations du monde à protéger leurs données et leur bien-être contre les cybermenaces plus présentes que jamais.

En 2003, Terranova Security commercialisait sa première solution de sensibilisation à la sécurité et, en 20 ans, l'entreprise a acquis une réputation redoutable. Aujourd'hui, elle représente un partenaire de choix mondial en sensibilisation à la sécurité, et son travail a été reconnu par le Market Guide 2020 de Gartner comme fournisseur de formation de sensibilisation à la sécurité assistée par ordinateur.

Terranova Security travaille de pair avec les organisations pour contribuer à changer les comportements afin de réduire le risque, en combinant efficacement éducation et technologie. L'éducation aide les personnes à participer activement aux développements professionnels et sociétaux, et la technologie favorise un environnement d'apprentissage beaucoup plus pertinent, durable et amusant. Terranova Security a remporté le prix de 2020 pour « Information Technology Educator of the Year GOLD WINNER - IT World Awards ».

Des sociétés internationales comme Microsoft se sont associées avec Terranova Security pour susciter des changements de comportements à long terme se fondant sur des programmes de formation ciblés, reproduisant la vie réelle, et offrant la qualité de contenu la plus élevée de l'industrie. Terranova Security travaille également avec des données sur l'hameçonnage par courriel de Microsoft afin que les utilisateurs bénéficient du matériel de formation le plus récent.

Les solutions de sensibilisation à la sécurité de Terranova Security procurent une foule d'avantages à tous ses clients et partenaires, notamment un soutien multilingue pour sa plateforme de sensibilisation à la sécurité, des simulations d'hameçonnage intuitives, et des outils de communication engageants et faciles à partager. L'entreprise a adopté une approche innovante et une démarche de consultation pour les services gérés et de personnalisation pour que chaque initiative de sensibilisation à la sécurité se moule aux besoins et objectifs des organisations.

Notes

Notes

GONE PHISHING TOURNAMENT™

Co-présenté par

TERRANOVA SECURITY

Microsoft