BEAUCERON
SECURITY

FORMATION ANTI-HAMEÇONNAGE 2021

LA FORMATION ANTI-HAMEÇONNAGE FONCTIONNE-T-ELLE?

Au cours des vingt dernières années, de nombreux programmes de sensibilisation à la sécurité ont été créés dans le but de partager des connaissances sur les concepts clés en cybersécurité.

Nous vivons dans un monde où chaque semaine les manchettes rapportent de nouvelles atteintes majeures à la protection des données ou de nouvelles attaques informatiques de taille; les gens sont donc plus conscients que jamais que la cybersécurité est un enjeu qui nécessite toute leur attention. Cependant, pour les professionnels de la sensibilisation à la sécurité, cet enjeu est passé d'un travail de sensibilisation à l'importance de la sécurité à la modification des comportements individuels ancrés et de la culture de sécurité dans les organisations. Alors que près de 85 % des violations de données malveillantes impliquent toujours des éléments humains de la cybersécurité[1], il est évident que même si les gens connaissent la cybersécurité, certains de leurs comportements les exposent toujours à certains risques.

Le problème persistant de l'hameçonnage, soit des attaques d'ingénierie sociale qui utilisent le courrier électronique pour atteindre les individus, est un bon exemple de cet enjeu.

Bien que les gens sachent souvent ce qu'est une attaque d'hameçonnage, ils ont en pratique bien du mal à éviter les pièges tendus par ce type d'attaque. Lorsque nous ajoutons à cela le fait que le volume d'attaques d'hameçonnage a doublé en 2020,[2] il est facile de constater qu'il est plus important que jamais de changer nos comportements lorsque nous utilisons la technologie.

Les programmes de formation anti-hameçonnage fonctionnent-ils?

Une préoccupation commune soulevée par certains professionnels de la cybersécurité concerne la question de l'utilisation de simulations d'hameçonnage par les organisations dans le cadre de leurs programmes de formation pour inciter les changements de comportement. De nombreux arguments ont été faits contre ce choix d'activité en évoquant le fait que ces programmes ne permettent pas d'atteindre un taux de clics de 0 %. Certains de ces arguments concernent aussi les conséquences émotionnelles de simulations d'hameçonnage mal exécutées qui peuvent aliéner ou mettre en colère des membres de l'équipe organisationnelle.

Cependant, comme le démontrent les conclusions de nos propres recherches, les programmes anti-hameçonnage sont un élément essentiel des efforts de cybersécurité de toutes les organisations. Ces programmes ne visent pas à atteindre un taux de clics de zéro, ils visent plutôt à créer des occasions d'apprentissage intéressantes qui permettent d'apprendre de l'expérience directe ou de démontrer facilement une connaissance adéquate de ce qu'est l'hameçonnage, en plus de motiver les employés à faire la bonne chose à ce sujet, en particulier pour signaler les menaces d'hameçonnage à l'organisation.

Nous démontrerons également comment les organisations peuvent minimiser les impressions négatives des employés en utilisant des méthodes de communications proactives, claires et efficaces combinées à une approche transparente et équitable de l'éducation et de l'hameçonnage.

Résumé des conclusions

Avons-nous toujours besoin de programmes anti-hameçonnage?

Plus de 75 % des organisations dans le monde ont déclaré avoir été confrontées à une attaque d'hameçonnage en 2020, [3]mais trop souvent encore, les programmes de formation anti-hameçonnage ne sont pas parmi les priorités des organisations.

Pour démontrer la valeur d'un programme de formation anti-hameçonnage bien conçu, nous avons analysé un ensemble de données de 4,3 millions de simulations d'hameçonnage envoyées à plus de 350 000 utilisateurs au sein de 325 organisations. Grâce à la plateforme Beauceron, ces organisations ont pu constater des améliorations rapides et continues à leurs cultures de la cybersécurité :

Après 90 jours ou plus	**Diminution de 85 % des clics** **Augmentation de 99 % des signalements** **Diminution de 11 % de l'indifférence**
Après deux ans ou plus	**Diminution de 90 % des clics** **Augmentation de 285 % des signalements** **Diminution de 37 % de l'indifférence**

Efficacité de notre méthode

Taux de clics

Le taux de clics est la mesure la plus couramment mentionnée dans les campagnes de sensibilisation à la sécurité. Ce taux indique combien d'employés réagissent aux tentatives d'hameçonnage. Lorsque la formation n'a pas eu lieu et que les utilisateurs sont ciblés par un hameçonnage à l'aveugle, les taux de clics se situent aux alentours de 30 %[4]. Il a été prouvé qu'éduquer les employés permet de diminuer la probabilité que ces derniers cliquent sur des courriels d'hameçonnage.[5]

Les organisations devraient donc s'efforcer de créer une base d'employés bien informés, ce qui se traduirait par un taux de clics inférieur à 5 %.
Bien que le taux de clics devrait être le plus bas possible, l'objectif d'une formation anti-hameçonnage ne devrait pas être de porter le taux de clics à 0 %.

Dans le monde réel, les attaquants utilisent des stratégies innovantes pour infiltrer les organisations, par exemple l'exploitation de sujets d'actualité, le ciblage des utilisateurs et la création de campagnes aléatoires et de courte durée. Ainsi, un taux de clics de 0 % peut indiquer que les simulations d'hameçonnage ne reflètent pas avec précision le type d'attaque réellement reçu par une personne.

L'objectif de la formation anti-hameçonnage ne devrait pas être d'augmenter le taux de clics à 0%.

BEAUCERON SECURITY

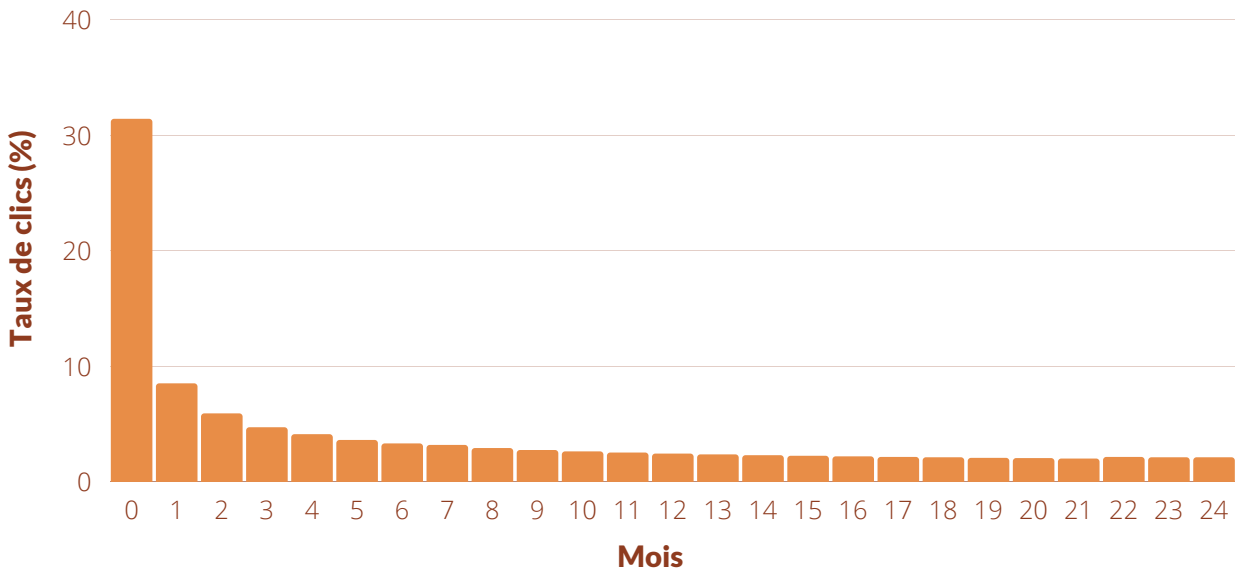
Afin d'obtenir un taux de clics représentatif pour votre organisation, il est préférable de tenir compte des éléments suivants :

- Randomiser les modèles pour contrôler le contenu et la difficulté d'hameçonnage
- Randomiser le moment où les simulations sont envoyées afin de contrôler des événements externes, par exemple l'heure de la journée, les discussions entre les employés.
- Envoyer des simulations d'hameçonnage sur une base régulière. Nous recommandons des simulations d'hameçonnage mensuelles pour contrôler les événements externes et fournir aux utilisateurs une formation continue.
- Envoyez des simulations d'hameçonnage à jour. Les tendances en matière d'hameçonnage changent régulièrement, c'est pourquoi vous devriez offrir à vos employés une formation qui imite des campagnes d'hameçonnage réelles afin de les rendre aussi résilients que possible.

Grâce à la plateforme Beauceron, les administrateurs peuvent tirer parti des capacités d'automatisation pour déterminer un taux de clics représentatif. Les résultats suivants démontrent les résultats rapides et durables que les organisations peuvent atteindre :

Tirez parti des capacités d'automatisation de la plateforme Beauceron pour voir des résultats rapides et durables.

- Immédiatement après la formation : 8,5 % (diminution de 73 %)
- Après 90 jours : 4,7 % (diminution de 85 %)
- Après deux ans : 2,1 % (diminution de 90 %)



*Le mois 0 est basé sur un taux d'hameçonnage aveugle moyen de l'industrie compris entre 30 et 40 %.

BEAUCERON SECURITY

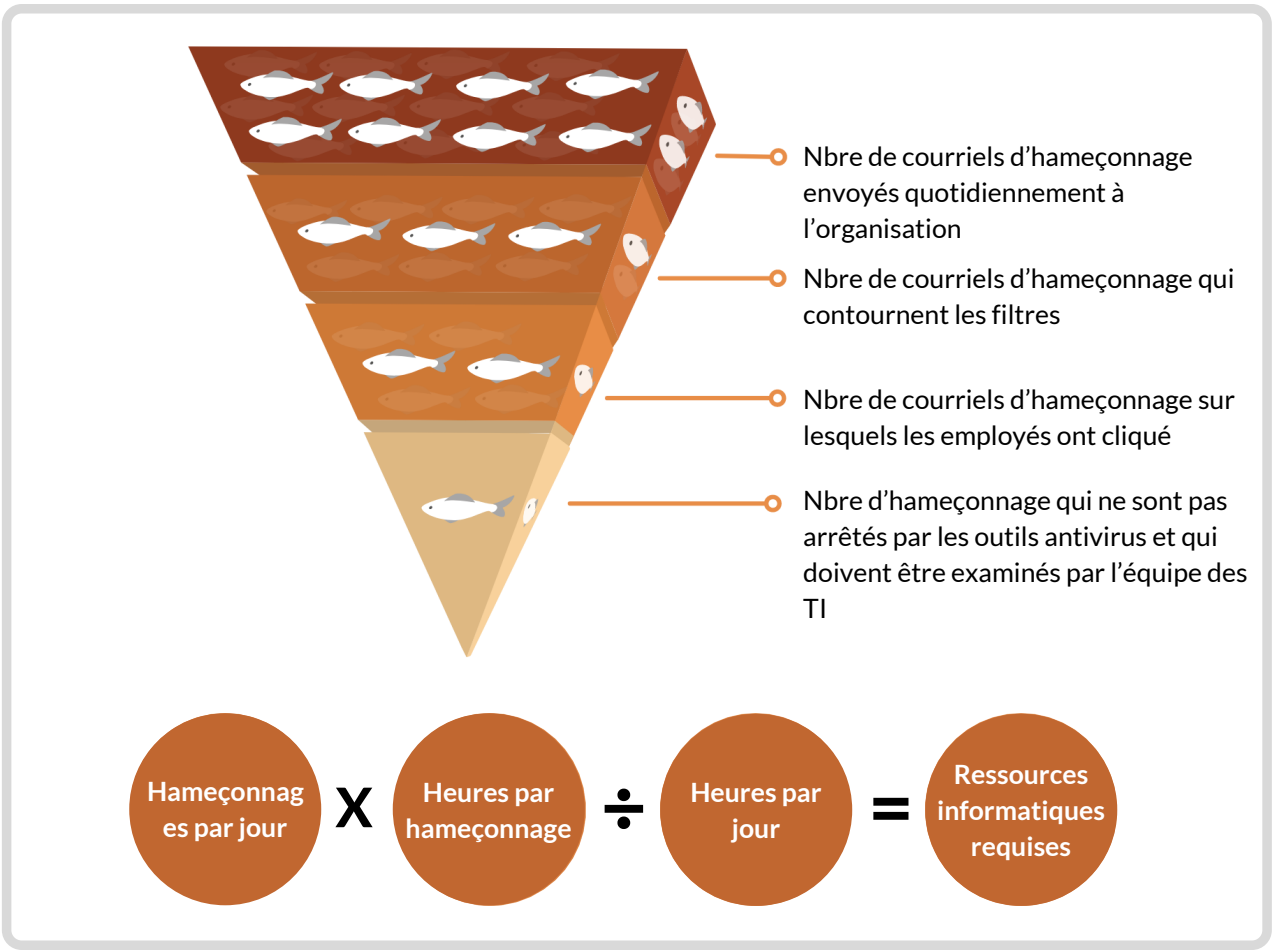
Le saviez-vous : Plus de 15 % des clics de phishing se produisent entre 8 h et 9 h ?

Tirer parti du taux de clics pour mesurer le retour sur investissement

Le taux de clics cible d'une organisation peut être déterminé en fonction de sa capacité à gérer les incidents en tenant compte de facteurs tels que le nombre de courriels malveillants reçus quotidiennement ou encore l'efficacité des solutions technologiques.

Établir une cible fournit une direction à l'équipe informatique, mais ce taux de clics ne prend cependant pas en compte les mesures proactives. Changer l'attitude et le comportement des employés permet à l'équipe informatique de devancer les menaces possibles tout en assurant une ligne de défense plus robuste et attentive.

Lors du calcul de la capacité de l'organisation, vous pouvez tirer parti des indicateurs clés de votre programme anti-hameçonnage :



Les mesures d'hameçonnage peuvent aider les organisations à mieux comprendre leur capacité d'hameçonnage.

BEAUCERON SECURITY

Relations avec les employés et l'équipe informatique

Cliquer sur une tentative d'hameçonnage peut susciter des émotions telles que la frustration, l'embarras ou la peur. Démarrer un programme de cybersécurité sur une note négative peut décourager les employés et nuire à l'instauration d'un milieu favorable à l'apprentissage dont les gens ont besoin pour changer et pour adopter de nouveaux comportements. Plutôt que de risquer que vos employés se sentent « trompés » par l'équipe des TI, nous recommandons que les administrateurs de la plateforme :

- Informent les employés du nouveau programme
- Forment les utilisateurs
- Communiquent clairement aux utilisateurs qu'ils recevront des simulations d'hameçonnage
- Définissent des attentes sur le nombre et la fréquence des simulations qu'ils recevront

Ces simples gestes permettront à l'équipe informatique et aux employés d'établir dès le départ une relation ouverte et transparente qui permettra d'établir une culture de cybersécurité.

L'hameçonnage à l'aveugle est effectué par certaines organisations afin de déterminer un taux de clics de contrôle. Ce taux de clics sert de base de référence à partir de laquelle les parties prenantes peuvent évaluer l'efficacité de la formation.

Bien que nous comprenions que certaines organisations souhaitent hameçonner à l'aveugle leurs utilisateurs, nous recommandons généralement de ne pas hameçonner à l'aveugle pour une meilleure relation informatique et employé.

Le taux de clics n'est pas la seule mesure qui compte

Le taux de clics a traditionnellement été utilisé pour évaluer les avantages des plateformes de sensibilisation à la cybersécurité, où le taux de clics sur des tentatives d'hameçonnage à l'aveugle sert de taux de clics de base à partir duquel les utilisateurs devraient s'améliorer grâce à la formation. Plusieurs études [5]ont démontré que le taux de clics devrait diminuer après la formation des employés. Ainsi, la nécessité de valider la diminution du taux de clics grâce à la formation a été réduite. Nous recommandons plutôt que les utilisateurs reçoivent une formation dès le premier jour afin que les organisations puissent se concentrer sur la création d'une base d'employés résilients.

La valeur de la plateforme peut toujours être déterminée par un taux de clics décroissant, mais les administrateurs doivent également chercher une plateforme qui permet d'encourager l'augmentation du taux de signalement et une diminution du taux d'indifférence. Ces mesures indiquent l'adoption de comportements et d'attitudes favorisant la cybersécurité et permettent aux équipes informatiques d'être proactives face aux menaces potentielles.

Le saviez-vous?77% des utilisateurs qui cliquent sur un hameçonnage le font dans les 24 heures suivant son arrivée dans leur boîte de réception.

Le taux de clics n'est qu'une mesure clé que les organisations devraient prendre en compte.

Taux de signalement

Le taux de signalement et le délai de signalement des tentatives d'hameçonnage sont des mesures clés pour évaluer le comportement des employés et la culture de la cybersécurité qui prévaut au sein de l'organisation. Les organisations doivent s'efforcer d'obtenir un taux de signalement élevé ainsi qu'un délai de signalement rapide. Ces taux indiquent que les employés sont bien informés, mais qu'ils sont également impliqués et qu'ils se soucient de jouer un rôle positif au sein de l'organisation.

Le signalement de tentatives d'hameçonnage permet aux équipes informatiques d'être proactives face aux menaces potentielles. Lorsqu'une tentative d'hameçonnage est signalée, les équipes informatiques peuvent faire enquête et déterminer si elle est malveillante. Ces courriels permettent également à l'équipe informatique de connaître le type de courriels capables de contourner leurs solutions technologiques. En se fondant sur les tendances évidentes des tentatives d'hameçonnage signalées, l'équipe informatique peut mettre à jour les filtres afin de réduire le nombre de courriels non détectés.

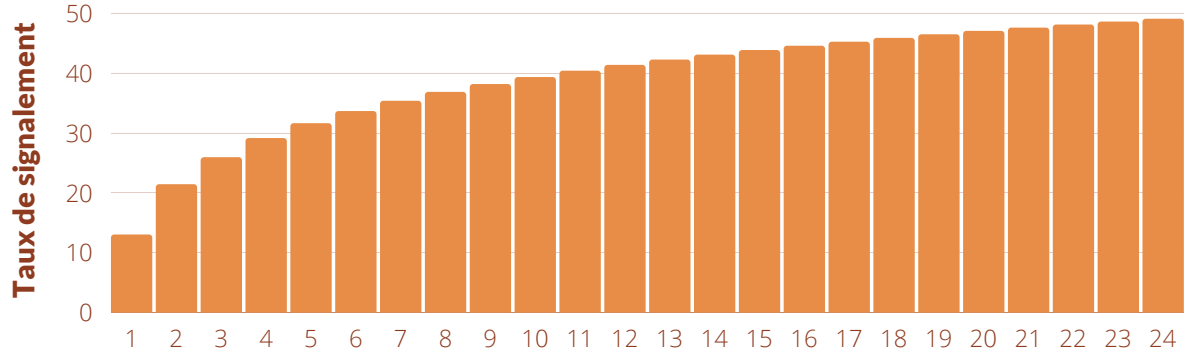
L'équipe informatique est également capable d'agir rapidement si une tentative d'hameçonnage est signalée après un clic dans le courriel. N'importe qui peut cliquer sur un lien dans un courriel d'hameçonnage au moment opportun, c'est pourquoi il est important d'encourager les employés à signaler les courriels d'hameçonnage, et ce même s'ils ont déjà cliqué dessus. L'équipe informatique a alors le temps de déterminer les répercussions de ce clic.

Afin d'assurer une culture proactive de la cybersécurité :

- Trouvez une solution qui facilite le signalement des courriels suspects, comme un bouton pour signaler les tentatives d'hameçonnage;
- Adoptez des solutions pour aider à détecter les menaces dans les courriels signalés. Le nombre de sites d'hameçonnage et de pourriels en circulation augmente, c'est pourquoi il est préférable d'utiliser des solutions qui permettent à l'équipe informatique de maximiser son temps;
- Communiquez l'importance d'une attitude ancrée dans la cybersécurité et mesurez le taux d'indifférence pour identifier les utilisateurs dont l'engagement pourrait être renouvelé.

Comme en témoigne une amélioration de 285 % des taux de signalement, les organisations ont eu beaucoup de succès dans la création d'une culture de cybersécurité positive en utilisant la plateforme Beauceron :

- Immédiatement après la formation : 13,0 %
- Après 90 jours : 25,8 % (amélioration de 99 %)
- Après deux ans : 49,1 % (amélioration de 285 %)



BEAUCERON SECURITY

Une culture proactive de la cybersécurité permet d'augmenter les taux de rapports jusqu'à 285 %.

Taux d'indifférence

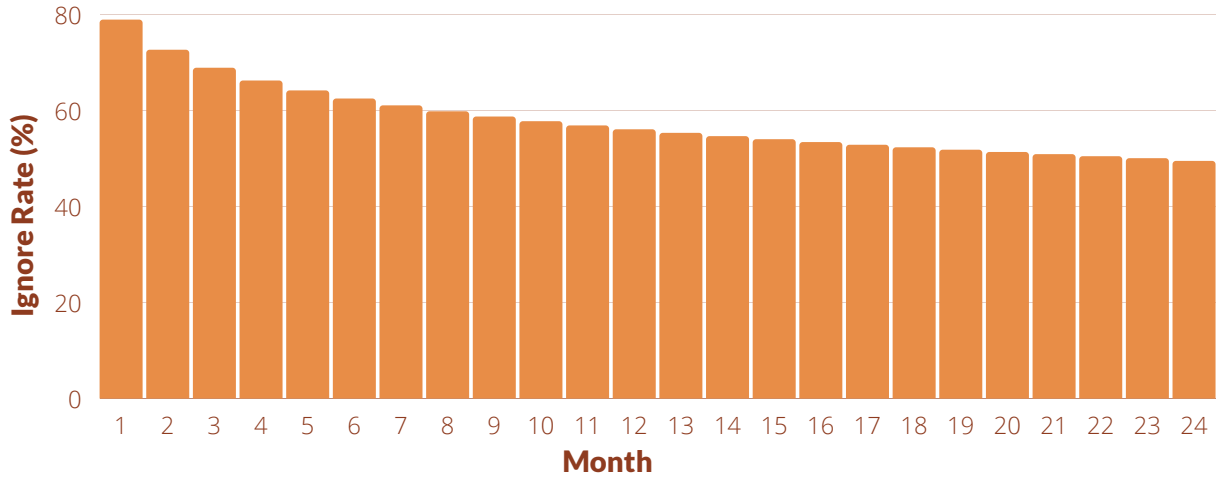
Lorsqu'il n'y a pas de clics sur les courriels d'hameçonnage ou que ceux-ci ne sont pas signalés, ils sont ignorés. Le taux d'indifférence aux simulations d'hameçonnage est une mesure importante, car celui-ci indique que les employés pourraient être désengagés ou avoir besoin d'une formation supplémentaire pour mieux reconnaître les tentatives d'hameçonnage.

Voici quelques facteurs à prendre en compte lorsque vous éduquez vos employés sur l'hameçonnage :

- Sollicitez la participation des employés avec des outils tels que des sondages pour comprendre s'ils savent à quoi ressemble une tentative d'hameçonnage et comment faire pour signaler une telle tentative.
- Planifiez une formation récurrente au moins une fois tous les 5 mois. La recherche a démontré qu'il s'agit du meilleur intervalle possible, même en étant optimiste sur la rétention des connaissances.[5] Cet intervalle de formation régulier permettrait également aux employés de se renseigner sur les tendances émergentes en matière d'hameçonnage. Les changements en matière d'hameçonnage peuvent être communiqués dans le matériel de formation, avec des exemples de menaces qui ont ciblé l'organisation. Les attaques réelles peuvent également être copiées (en supprimant les liens malveillants) afin de les utiliser lors de simulations d'hameçonnage pour améliorer directement la résilience des employés.
- Lors de la prestation de la formation, tentez de contextualiser l'information. Expliquer le « pourquoi » aux employés les aide à comprendre le rôle important qu'ils jouent dans la ligne de défense, ce qui peut changer leur attitude envers la cybersécurité et ainsi augmenter l'efficacité de la formation[6].

Grâce à la plateforme Beauceron, les utilisateurs peuvent réduire le taux de tentatives d'hameçonnage ignorées de près de 37 % :

- Immédiatement après la formation : 78,8 %
- Après 90 jours : 70,0 % (diminution de 11 %)
- Après deux ans : 49,5 % (diminution de 37 %)



La diminution du taux d'ignore de 37% indique une augmentation des niveaux de sensibilisation et d'éducation.

BEAUCERON SECURITY

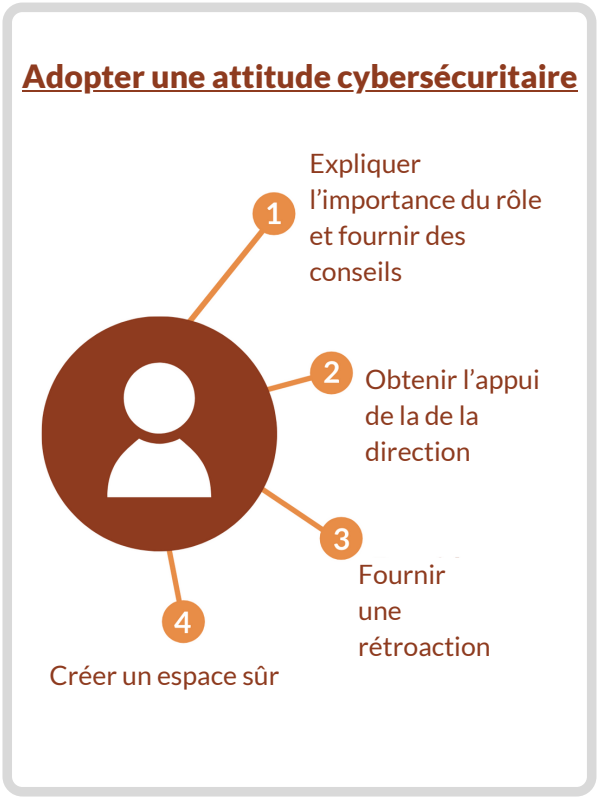
Si les employés n'ont pas encore adopté une attitude ancrée dans la cybersécurité :

1. Aidez-les à comprendre le rôle important qu'ils jouent dans la ligne de défense de l'organisation

- Expliquez comment le signalement des tentatives d'hameçonnage permet à votre organisation d'enquêter plus rapidement sur les menaces potentielles et l'effet positif que ces comportements ont sur l'organisation.
- Fournissez aux employés des conseils en matière de cybersécurité qu'ils peuvent utiliser à la fois sur le lieu de travail et à la maison, afin qu'ils comprennent la pertinence de la formation en cybersécurité.

2. Parlez ouvertement de l'appui de l'organisation et de la direction envers la cybersécurité

- Montrez l'engagement des dirigeants et encouragez les dirigeants à discuter régulièrement de l'importance de la cybersécurité avec les employés.
-



3. Offrez des rétroactions

o Célébrez la réussite des utilisateurs lorsqu'ils s'impliquent dans le programme de cybersécurité. Cela pourrait prendre la forme d'un message de remerciement aux utilisateurs qui ont signalé toutes les simulations d'hameçonnage, souligner les utilisateurs qui ont engagé une conversation sur la cybersécurité ou donner une carte-cadeau à l'utilisateur qui a la cote de risque le plus faible.

4. Créez un espace sûr

o Assurez-vous de bien faire comprendre à tous que n'importe qui est susceptible de cliquer sur un lien dans un courriel d'hameçonnage si la personne le reçoit au moment opportun. Bien qu'il soit important de réduire le nombre de clics sur les courriels d'hameçonnage, il est encore plus important de signaler les tentatives d'hameçonnage, même après avoir cliqué sur celles-ci. Ces simples gestes peuvent permettre aux membres de l'organisation de se sentir à l'aise d'admettre leur erreur après l'avoir commise afin de permettre à l'équipe informatique d'enquêter plus rapidement.

Notre approche

Chez Beauceron Security, notre mission est de changer la conversation sur la sensibilisation et de donner aux gens les moyens de se sentir en contrôle de la technologie qu'ils utilisent et sur laquelle ils comptent quotidiennement. La plateforme infonuagique de Beauceron permet aux organisations et aux particuliers de changer leurs comportements à risque en matière de cybersécurité. Notre plateforme sollicite la participation des utilisateurs, favorise leur apprentissage et les aide à reconnaître le rôle qu'ils ont à jouer dans la cybersécurité, en plus d'aider les organisations à créer et à maintenir une culture de sécurité positive.
Les professionnels de la sécurité de Beauceron, chefs de file sur le marché, invitent les professionnels de la sécurité à consacrer leur temps à ce qui compte le plus, c'est-à-dire d'engager un dialogue avec les employés et faire progresser les objectifs de leur programme de sécurité stratégique.
Voici quelques fonctionnalités clés de notre plateforme qui vous aideront à faire de votre programme de cybersécurité un succès :

Fonctionnalités

Voici quelques fonctionnalités clés qui vous aideront à faire de votre programme de cybersécurité un succès :

Tableau de bord personnel

Pour favoriser un changement de comportement, chaque utilisateur dispose d'une cote de risque personnelle sur la plateforme. Cette cote est accordée selon le degré de sensibilisation, le niveau d'exposition, les incidents et les récompenses reçues. La cote de risque des utilisateurs diminue à mesure qu'ils présentent des comportements positifs, par exemple signaler des simulations d'hameçonnage à l'aide du bouton de signalement des tentatives d'hameçonnage. Non seulement ces comportements positifs sont soulignés par leur cote de risque personnelle, mais aussi par des écussons et un tableau de classement sans prétention.

Formation

La première chose que nous entendons sur le terrain est qu'une grande quantité de contenu uniformisé n'est pas aussi précieuse qu'un contenu pertinent personnalisé. Il peut être difficile d'obtenir l'appui des employés s'ils ne peuvent établir une connexion avec le matériel d'apprentissage.
C'est pour cette raison que Beauceron comprend un répertoire de contenu bilingue qui peut être automatiquement attribué à des individus ou à des groupes, de façon proactive, ou encore réactive après un incident. Des formations peuvent également être mises à la disposition des employés pour leur permettre de s'y inscrire.
Permettre aux employés de s'inscrire eux-mêmes à des modules de formation en matière de sécurité est à la fois un excellent moyen de fournir une éducation pertinente pour la vie familiale d'un employé (médias sociaux, etc.) et identifier de manière proactive des candidats potentiels dans l'organisation qui peuvent avoir un intérêt ou des compétences en cybersécurité.

Renforcement du comportement

L'équipe de sécurité peut tirer parti de Beauceron pour attribuer des récompenses ou des incidents et y attacher une formation corrective, si souhaité. Cette fonctionnalité permet à l'équipe de sécurité de renforcer les comportements positifs et de faire un suivi auprès des employés pour leur expliquer comment éviter de futurs incidents.

Phishes

Simulations

Notre plateforme aide les organisations à aller au-delà des taux de clics des campagnes d'hameçonnage avec des informations plus approfondies pour permettre aux employés de repérer et de signaler les cyberrisques. Beauceron fournit une variété de simulations d'hameçonnage automatisées qui peuvent facilement être personnalisées pour répondre aux besoins de l'organisation. Les organisations peuvent configurer des simulations automatisées et aléatoires pour qu'elles s'exécutent sur une base bihebdomadaire, mensuelle ou trimestrielle. La configuration permet aussi de planifier manuellement des campagnes spécifiques ou de les lancer sans donner de formation supplémentaire. Avec l'outil d'édition de Beauceron, les organisations peuvent facilement personnaliser ou créer leurs propres simulations d'hameçonnage.
Une fois mis en œuvre, vous pouvez considérer que les simulations d'hameçonnage et la formation corrective sont en mode automatique.
Les simulations sont insérées directement dans la cote de risque individuelle. Lorsqu'ils signalent une simulation, les employés sont automatiquement récompensés pour leurs comportements positifs en sécurité.

Détection des menaces réelles

Afin de réduire la charge de travail de votre équipe de sécurité, votre organisation peut tirer parti de Beauceron Analyst en tant que service complémentaire offert avec PhishForward. L'outil Analyst extrait des données sur les menaces provenant de plusieurs sources externes et attribue une note aux courriels en fonction des métadonnées contenues dans ces derniers, y compris l'identification ou la reconnaissance d'expéditeurs potentiellement malveillants, de liens malveillants ou de pièces jointes suspectes. L'outil Analyst établira alors si le courriel est probablement malveillant ou non. Les seuils configurables pour la notation vous permettent de personnaliser la sensibilité de l'outil d'analyse des courriels.

Conclusion

Chez Beauceron, nous avons démontré que les programmes anti-hameçonnage qui sont entièrement intégrés à une plateforme de changement de comportement positif sont un moyen efficace de réduire les risques et d'engager les employés.
Notre plateforme peut alimenter des programmes de sensibilisation à la sécurité et de changement de comportement de classe mondiale qui fourniront à votre organisation de meilleurs résultats, et ce plus rapidement.

BEAUCERON SECURITY

La plateforme Beauceron fournit des simulations d'hameçonnage personnalisées et la détection des menaces pour assurer votre sécurité et la sécurité de votre organisation.

Une approche positive

Chez Beauceron Security, notre mission est de changer la conversation sur les cyberrisques et de donner aux gens les moyens de se sentir en contrôle de la technologie qu'ils utilisent.
Nous avons créé une puissante plateforme de logiciel-service pour aider les organisations à faire face aux cyberrisques. Notre plateforme complète fonctionne grâce à des programmes de sécurité qui favorisent les changements de comportement. Nous engageons les utilisateurs, favorisons leur apprentissage et les aidons à reconnaître le rôle qu'ils ont à jouer dans la cybersécurité.
Le haut degré d'automatisation utilisé par Beauceron permet aux organisations de gagner des milliers d'heures de travail tout en fournissant à la direction des données analytiques en temps réel afin d'avoir rapidement une vue d'ensemble sur la conformité aux normes de cybersécurité.
Fondée en 2016 par des professionnels de la sécurité, Beauceron Security sert des organisations dans tous les principaux secteurs de l'industrie avec des clients de toutes tailles, de petites PME à 10 employés à des organisations comptant plus de 100 000 employés.

Alors commençons!

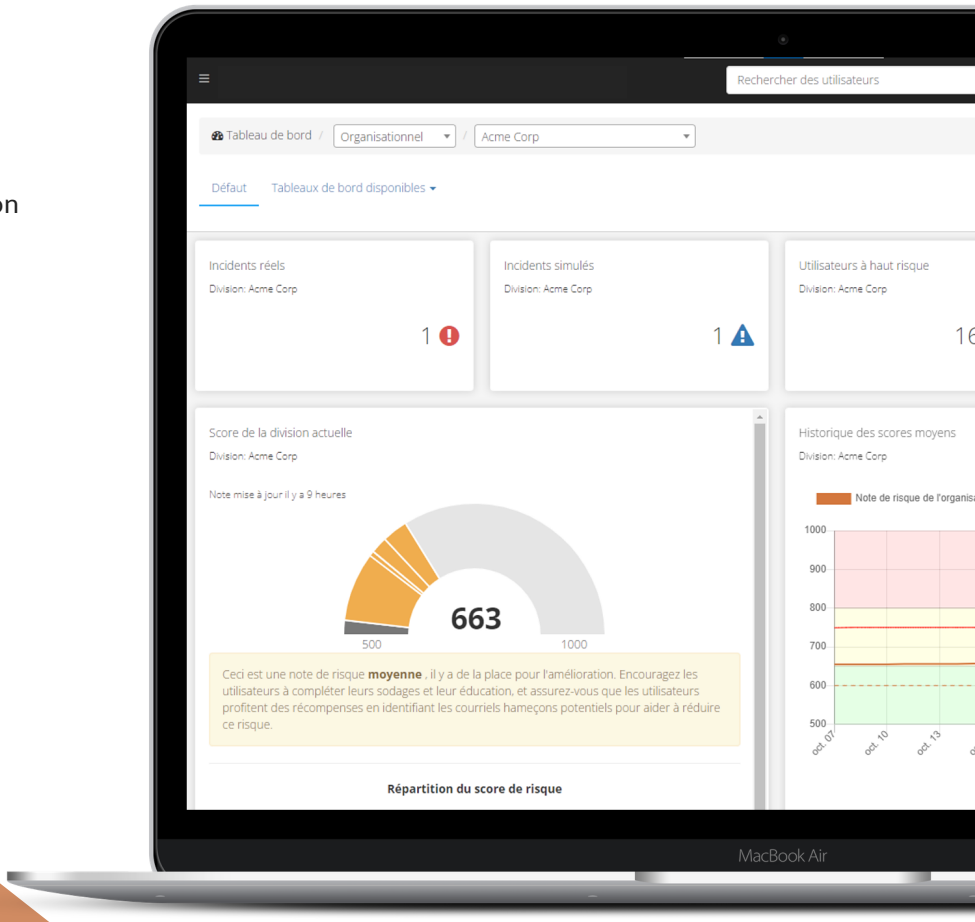
Simplifiez l'intégration de vos utilisateurs, obtenez des rapports de conformité en temps réel et créez du contenu personnalisé et pertinent en une fraction du temps que vous consacriez à ces tâches.

Votre temps est précieux, mettez-le là où il compte le plus : impliquer votre communauté.

Notre équipe de réussite client est prête à vous aider à atteindre ces résultats.

Contact Us

Tél. bureau : +1 (877) 516-9245
sales@beauceronsecurity.com
527, rue Queen, bureau 110, Fredericton (N.-B.), Canada



BEAUCERON SECURITY

References

[1] Verizon, "2021 Data Breach Investigations Report," 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. [Accessed 2021].

[2] APWG, "Phishing Activity Trends Report," 2021. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf. [Accessed 2021].

[3] FBI, "2020 Internet Crime Report," 2020. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. [Accessed 2021].

[4] D. Jampen, G. Gur, T. Sutter and B. Tellenbach, "Don't click: towards an effective anti phishing training. A comparative literature review," Human-centric Computing and Information Sciences, vol. 10, no. 1, pp. 1-41, 2020.

[5] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Computers & Security, vol. 42, pp. 165-176, 2014.