proofpoint.

EBOOK

Mesurer l'efficacité de la sensibilisation à la sécurité informatique pour une protection durable

Guide à l'attention des RSSI et des responsables informatiques

proofpoint.com/fr

Introduction

Cette nouvelle décennie a plongé les responsables informatiques et de la sécurité dans un tourbillon de défis et de changements. Qu'il s'agisse des difficultés liées à l'adoption du télétravail pendant la pandémie ou de la multiplication des attaques de phishing cherchant à profiter de la situation, l'année 2020 a marqué le début d'une nouvelle ère pour la cybersécurité.

Dans une enquête récente réalisée auprès de professionnels de la technologie, 57 % ont déclaré que leur entreprise avait été victime d'une attaque de phishing fructueuse en 2020, contre 55 % l'année précédente[2]. Et la situation ne s'arrange pas. Face à la multiplication des attaques de ransomwares et des compromissions de données très médiatisées, les entreprises se voient contraintes de limiter les risques auxquels elles sont exposées.

Les compromissions sont une véritable catastrophe pour les victimes, mais elles peuvent faire naître des conversations plus que nécessaires parmi les dirigeants et au sein du conseil d'administration à propos de la cybersécurité et du rôle que joue le comportement des utilisateurs dans la protection de l'entreprise.

La plupart des cybermenaces nécessitent une activation quelconque de la part des utilisateurs. C'est pourquoi des programmes efficaces de sensibilisation à la sécurité informatique, ainsi que des changements dans le comportement des utilisateurs, peuvent jouer un rôle déterminant dans la réduction des risques[3]. De nombreux responsables de la sécurité en sont bien conscients. Mais il n'est pas toujours aussi évident de mesurer et d'expliquer l'impact de votre programme de sensibilisation à la sécurité informatique aux dirigeants.

Cet eBook s'intéresse aux tenants et aboutissants des programmes de sensibilisation à la sécurité informatique conçus pour assurer une protection durable de l'entreprise. Il présente des stratégies permettant d'obtenir, de mesurer et de conserver l'adhésion des parties prenantes, et explique comment tirer le meilleur parti de cet investissement essentiel.

85 %

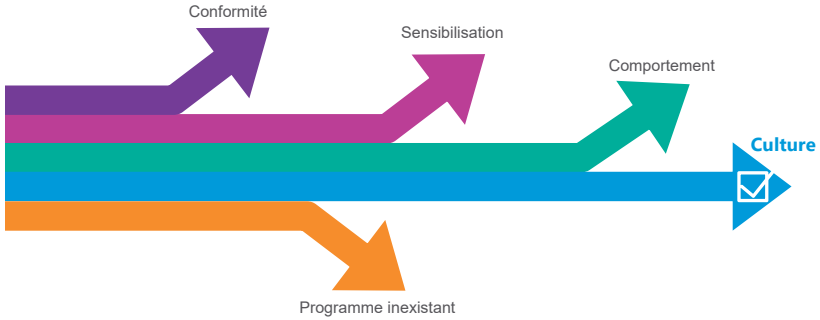
des directeurs financiers travaillant aux États-Unis ont indiqué que leur conseil d'administration a eu une discussion formelle à propos des récentes attaques de cybersécurité et de la suite des événements[1].

[1] CNBC, « CNBC Global CFO Council Survey » (Enquête menée par le conseil mondial des directeurs financiers de CNBC), juillet 2021
[2] Proofpoint, « State of the Phish 2021 », février 2021
[3] Proofpoint, « Protéger l'utilisateur final », février 2019

L'importance de la sensibilisation à la sécurité informatique

La sensibilisation à la sécurité informatique n'est pas une priorité budgétaire par rapport aux contrôles techniques. Mais ce n'est pas une fatalité. Avec des indicateurs convaincants et un argumentaire efficace, vous pouvez atteindre deux objectifs clés : réduire les risques de manière tangible et montrer aux RSSI et aux autres parties prenantes pourquoi la sensibilisation à la sécurité informatique est indispensable pour protéger l'entreprise.

Les préoccupations de la direction sont fonction de l'état et des objectifs du programme de sécurité en place. Par exemple, les programmes orientés conformité se concentrent sur le respect des normes. L'efficacité des programmes orientés comportement est quant à elle évaluée en fonction d'indicateurs tels que le taux de clics et le taux de signalement dans le cadre des simulations de phishing.



Niveaux de maturité des programmes de sensibilisation à la sécurité informatique

Processus d'instauration d'une culture de la cybersécurité

La grande majorité des entreprises (98 %) disposent d'un programme de sensibilisation à la sécurité informatique[4]. Pourtant, 64 % d'entre elles organisent uniquement des sessions de formation formelles (en personne ou en ligne) et passent à côté d'autres opportunités de renforcement de la sensibilisation à la sécurité. Seuls 23 % utilisent tous les types de supports disponibles (évaluations, formations et communications).

Une formation continue s'appuyant sur un large éventail de canaux permet d'améliorer l'ancrage des connaissances ainsi que les résultats en matière de sensibilisation à la sécurité informatique. C'est pourquoi nous recommandons vivement aux entreprises d'utiliser un maximum de canaux.

L'une des clés pour renforcer la sensibilisation à la sécurité consiste à instaurer une culture qui convainque les utilisateurs qu'un niveau de sécurité élevé est bénéfique non seulement pour l'entreprise, mais aussi pour eux personnellement. Pour y parvenir, vous pouvez combiner différentes activités visant à renforcer la sensibilisation, à modifier les comportements et à encourager les collaborateurs à combattre les cybercriminels. Pour cela, vous devez proposer en permanence (et non une ou deux fois par an) des formations pertinentes et utiles pour les utilisateurs.

Approches actuelles de la sensibilisation à la sécurité informatique[5] :

29 %
Simulations d'attaques de phishing uniquement

41 %
Sessions de formation formelles uniquement

7 %
Contenu informatif uniquement

23 %
Combinaison de types de contenu

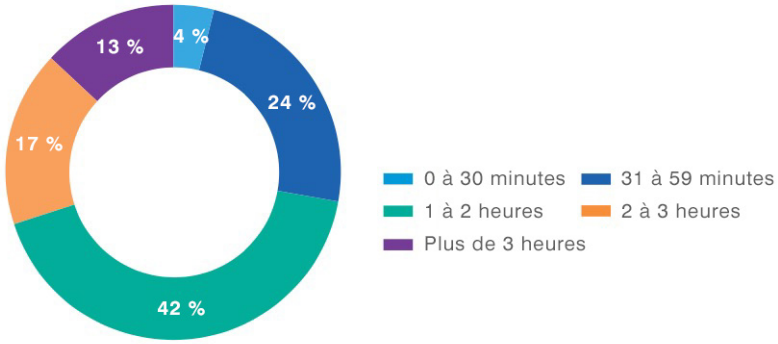
[4] Proofpoint, « State of the Phish 2021 », février 2021
[5] Ibid

Comment élaborer un programme efficace

Plus une entreprise consacre de temps à son programme de sensibilisation à la sécurité informatique, plus elle a de chances qu'il soit efficace.

Temps consacré par les entreprises à la sensibilisation à la sécurité informatique

La plupart des entreprises consacrent moins de deux heures par utilisateur et par an à la sensibilisation de leurs collaborateurs.



Chaque année, de plus en plus d'entreprises augmentent la fréquence de leurs activités de sensibilisation à la sécurité informatique.

Centrez les efforts de formation sur les utilisateurs vulnérables

Il est possible que vos tentatives pour étendre votre programme de sensibilisation à la sécurité informatique suscitent une résistance. Les plus sceptiques peuvent craindre que le programme n'alourdisse la charge de travail d'un trop grand nombre d'utilisateurs, en particulier ceux qui ne présentent pas un risque élevé.

Pour dissiper certaines inquiétudes, envisagez de centrer plus régulièrement vos efforts de formation sur les utilisateurs vulnérables, plutôt que d'adopter une approche générique imposant davantage de formations à l'ensemble du personnel. Avec une approche ciblée, les parties prenantes savent que les sessions de formation supplémentaires et les efforts de sensibilisation à la sécurité informatique sont justifiés. Et les utilisateurs comprennent pourquoi ils y sont soumis.

D'autres se préoccupent davantage du temps consacré à la formation que du nombre de personnes concernées. Heureusement, il existe des moyens de renforcer la sensibilisation des utilisateurs sans pour autant leur faire perdre du temps.

Envisagez d'avoir recours à des newsletters, des réunions-débats, des pages de wiki et des notifications par email pour sensibiliser vos utilisateurs à la sécurité informatique sans qu'ils n'y passent trop de temps.

Savez-vous qui sont vos utilisateurs les plus vulnérables ?

Chez Proofpoint, nous utilisons l'acronyme VAP (Very Attacked People™, ou personnes très attaquées) pour désigner la catégorie d'utilisateurs que les cybercriminels ciblent avec une intensité inhabituelle : volumes élevés d'attaques, menaces extrêmement ciblées, tactiques sophistiquées, ou les trois à la fois. Si tous les utilisateurs sont des cibles potentielles, les VAP présentent une valeur inestimable en raison de leurs contacts professionnels uniques et de leur accès privilégié aux données, systèmes et autres ressources.

Les VAP sont **3 à 12** fois plus ciblés que les autres utilisateurs.

D'après nos observations, les VAP ne sont pas toujours les VIP d'une entreprise, tels que les cadres dirigeants. Ils peuvent par exemple faire partie des départements des ressources humaines, des relations publiques, du marketing ou de la recherche. N'importe quel collaborateur bénéficiant d'un accès adéquat peut être une cible de grande valeur.

Une fois que vous avez identifié les VAP, il est essentiel de combler leurs lacunes en matière de cybersécurité au moyen de formations extrêmement ciblées. Vous pouvez par exemple envoyer des simulations d'attaques de phishing aux VAP ciblés par le phishing d'identifiants de connexion. S'ils se laissent piéger, proposez-leur une formation facultative. Cette approche ciblée permet de réduire les risques liés aux personnes sans faire perdre de temps aux utilisateurs non concernés.

La sensibilisation à la sécurité informatique est un processus qui s'inscrit dans la durée. Vous devez organiser des formations complètes et continues permettant aux utilisateurs de se tenir au fait du paysage des menaces en constante évolution. Ce processus comprend les éléments suivants :

- Évaluations régulières
- Formations
- Activités de renforcement
- Mesures

Pour garder le rythme et tenir les parties prenantes informées, envisagez de créer un planning reprenant les activités, canaux, messages et thèmes de votre programme.

Mesurer l'efficacité de la sensibilisation à la sécurité informatique

Bon nombre d'entreprises évaluent l'efficacité de leurs programmes en se basant uniquement sur les sessions de formation suivies (à des fins de conformité) et sur le pourcentage d'utilisateurs qui se laissent piéger par des simulations d'attaques. Mais pour véritablement modifier le comportement des utilisateurs et réduire les risques, vous devez aller encore plus loin.

Pour ce faire, vous pouvez notamment établir des profils de risque plus complets. Voici quelques indicateurs clés permettant d'évaluer l'impact réel des programmes de sensibilisation à la sécurité informatique :

Taux de signalement dans les simulations

Cet indicateur fournit des informations sur les utilisateurs qui ne se contentent pas d'éviter les attaques et se montrent proactifs en adoptant les bons comportements et en mettant en pratique ce qu'ils ont appris pendant les formations de sensibilisation à la sécurité lorsqu'ils détectent quelque chose de suspect.

Taux de clics réel

La solution de protection avancée de la messagerie de Proofpoint vous permet de connaître le taux de clics sur des contenus dangereux, même si l'URL est bloquée ou réécrite pour des raisons de sécurité. Cet indicateur permet d'évaluer les connaissances concrètes des utilisateurs. Grâce à ces données, vous pouvez déterminer si les utilisateurs s'améliorent sur le plan de la détection des contenus dangereux.

Types de messages signalés

À l'aide d'un module d'extension, les utilisateurs peuvent signaler les contenus suspects, comme ils le feraient avec une boîte email de signalement d'abus. Proofpoint Targeted Attack Protection (TAP) vous montre comment différents types d'emails ont été classés (malveillants, spam, faible risque, etc.). Vous pouvez évaluer la progression des utilisateurs au fil du temps en ce qui concerne le signalement des messages qui pourraient mettre l'entreprise en péril.

Impact réel

Cet indicateur est le plus important de tous. Il mesure l'impact des formations sur les utilisateurs en vous indiquant s'il y a eu une réduction du nombre d'attaques de phishing fructueuses, de compromissions d'identifiants de connexion, d'incidents d'origine interne et de malwares. Il s'agit de la mesure d'excellence ultime. En outre, cet indicateur est indispensable pour obtenir l'adhésion à long terme des parties prenantes à l'égard des programmes de sensibilisation à la sécurité informatique.

Réponse à la question : Quels devraient être nos taux de clics et de signalement ?

Recommandations de Proofpoint :

< 5 %
Taux d'échec/ de clics

> 70 %
Taux de signalement

Communiquer efficacement avec votre RSSI et les principales parties prenantes

Les arguments ayant trait à la peur ambiante, aux doutes et aux incertitudes ne vous mèneront pas bien loin auprès de la direction et des parties prenantes. Oui, les cybermenaces doivent être gérées. Mais en abusant des tactiques jouant sur la peur et en exagérant les menaces, vous risquez de créer un scénario classique du garçon qui criait « Au loup ! » qui vous dessert plus qu'il ne vous sert.

Stratégies clés pour communiquer sur les performances des programmes de sensibilisation à la sécurité

Quantité

Le contexte est important. C'est pourquoi il est essentiel de comprendre vos performances globales et votre positionnement par rapport aux autres entreprises. Pour vous comparer à vos concurrents, concentrez-vous sur des indicateurs positifs plutôt que sur des indicateurs négatifs tels que le taux de clics lors des simulations.

Exemples d'indicateurs positifs :

- Augmentation des taux de signalement par les utilisateurs lors des simulations d'attaques de phishing
- Améliorations des résultats des évaluations des connaissances en matière de sécurité informatique
- Augmentation de la précision des messages malveillants signalés par les utilisateurs
- Hausse des taux de participation des utilisateurs aux activités de sensibilisation à la sécurité informatique

Qualité

Les récits, combinés avec des données, contribuent à démontrer que la sensibilisation à la sécurité informatique est bien plus qu'une activité de conformité imposée, qu'elle modifie les comportements des utilisateurs et qu'elle fait évoluer activement la culture de l'organisation dans la mesure où les utilisateurs comprennent mieux les risques et participent à la protection de l'entreprise.

Exemples de récits :

- Un utilisateur a neutralisé une attaque de phishing sophistiquée réelle.
- Des utilisateurs ont formulé des commentaires positifs concernant le programme de sensibilisation dans une enquête de satisfaction.
- Un membre de l'équipe de direction ou un collaborateur connu a partagé des informations avec le personnel concernant la sensibilisation à la sécurité informatique.

Visibilité sur la sensibilisation à la sécurité informatique via un tableau de bord

La sensibilisation à la sécurité informatique constitue l'une des principales mesures à prendre pour protéger votre entreprise. C'est l'une des raisons pour lesquelles nous avons conçu le tableau de bord du RSSI. Il permet aux équipes informatiques et de sécurité d'accéder aux principaux indicateurs qui prouvent que les programmes de cybersécurité induisent des changements de comportement et favorisent l'instauration d'une culture de la sécurité. Ces indicateurs de réussite mettent en évidence le retour sur investissement et plaident en faveur d'un futur investissement.

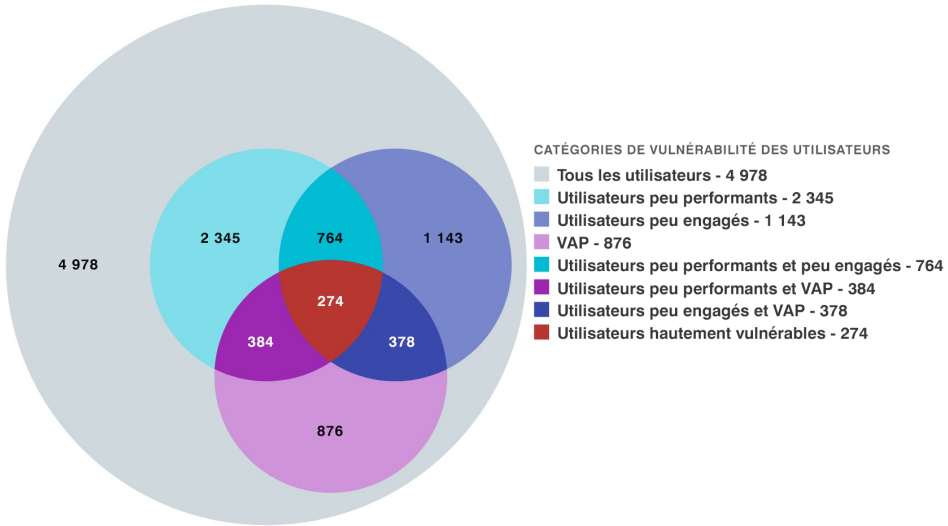
Le tableau de bord du RSSI de Proofpoint vous permet d'accéder à des indicateurs tels que la vulnérabilité des utilisateurs et le score de votre programme de sécurité informatique.

Vulnérabilité des utilisateurs

Identifiez les utilisateurs peu performants et peu engagés, ainsi que ceux qui cliquent sur des messages malveillants. Si les utilisateurs sont identifiés en tant que VAP par Proofpoint Targeted Attack Protection, ces données sont intégrées pour obtenir un meilleur aperçu du profil de risque global de ces utilisateurs.

274 utilisateurs hautement vulnérables (sur un total de 4 978 utilisateurs)

82 utilisateurs hautement vulnérables de moins au cours des 90 derniers jours

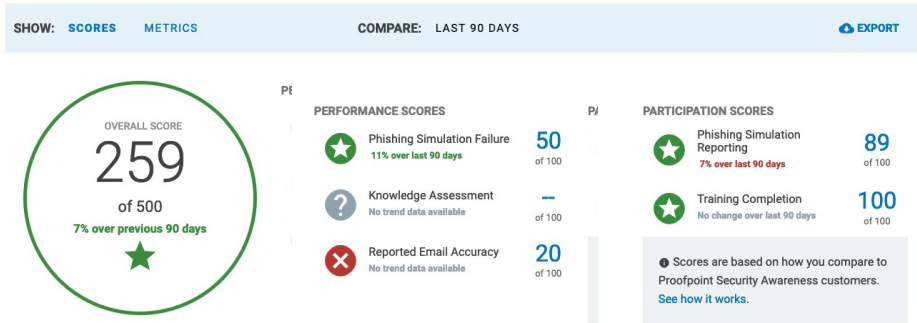


Score du programme de cybersécurité

Les scores de performances et de participation montrent à quel percentile vous correspondez dans chaque domaine, ainsi que l'évolution du score global. Les icônes de type feux de signalisation vous permettent d'identifier en un clin d'œil les domaines dans lesquels le programme doit être amélioré.

Récapitulatif des scores du programme de cybersécurité

Suivez les performances de votre programme de cybersécurité au fil du temps grâce au score du programme. Cliquez sur chaque score pour voir comment il a été calculé.



Récapitulatif de la vulnérabilité des utilisateurs dans le tableau de bord du RSSI

Visibilité sur la sensibilisation à la sécurité informatique via un tableau de bord

Comparaison du percentile au fil du temps

En association avec le score du programme de cybersécurité, découvrez le percentile auquel vous correspondez par rapport aux autres entreprises du secteur à des fins d'analyse. Vous pouvez ainsi évaluer vos progrès au fil du temps.

Les attaques d'aujourd'hui ciblent les personnes, pas seulement les technologies. C'est pourquoi une approche efficace et centrée sur les personnes de la protection de votre entreprise nécessite des formations ciblées qui font de la cybersécurité une priorité, en particulier pour les utilisateurs vulnérables et les VAP.

Le tableau de bord du RSSI vous permet d'accéder aux indicateurs nécessaires pour optimiser la sensibilisation à la sécurité informatique. Il n'a jamais été aussi simple de communiquer avec votre RSSI, de conserver l'adhésion des parties prenantes et d'optimiser votre programme.

Pour découvrir comment Proofpoint peut vous aider à modifier le comportement des utilisateurs et faire de la cybersécurité un élément essentiel de votre culture d'entreprise, consultez le site proofpoint.com/fr.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0504-002-01-01 09/21