Comment Proofpoint Security Awareness Training stimule l'engagement des utilisateurs

Favoriser les habitudes saines en matière de cybersécurité pour réduire les risques

Produits

- Proofpoint Security Awareness Training
- Proofpoint Targeted Attack Protection

Avantages

- Captez l'attention des utilisateurs en proposant des formations ciblées qui tiennent compte des lacunes de chacun en termes de connaissances.
- Déployez un programme de formation qui trouve un écho auprès d'un public international, avec des contenus adaptés à la langue et à la culture des utilisateurs.
- Motivez les utilisateurs à intégrer leurs acquis dans leur pratique quotidienne grâce à des modules de microapprentissage courts, qui leur sont proposés régulièrement.

Préserver l'intérêt des utilisateurs dans le cadre d'un programme de sensibilisation à la sécurité informatique est une véritable gageure. Ils sont fortement sollicités, tant à titre professionnel que dans leur sphère privée. Et comme un grand nombre d'entreprises n'affectent que deux heures par an, voire moins, à la formation des utilisateurs, les professionnels de la sécurité n'ont pas le temps d'exercer une réelle influence sur leur comportement. Pour les entreprises ayant une présence mondiale, les innombrables différences culturelles et linguistiques au sein de la base utilisateurs ajoutent encore une couche de complexité.

Proofpoint Security Awareness Training peut vous aider à relever ces défis. Ce programme est conçu pour capter et conserver l'attention des utilisateurs, tout en favorisant l'adoption à long terme d'habitudes de cybersécurité qui les protègent eux-mêmes autant que votre entreprise. Nous vous aidons à identifier les utilisateurs qui ont besoin d'attention supplémentaire. De même, notre solution vous permet d'étendre et de développer votre programme pour que vous puissiez établir une culture de la sécurité forte, qui stimule les changements de comportements.

Proofpoint adopte une approche globale de la formation de sensibilisation à la sécurité informatique. Notre cadre ACE (Assess, Change behavior, Evaluate) s'articule en trois phases : l'évaluation de l'état actuel de votre solution de sécurité, la modification des comportements et l'évaluation des résultats. Cette approche vous permet à la fois de stimuler les changements de comportements et d'améliorer votre programme de sensibilisation à la sécurité informatique au fil du temps.

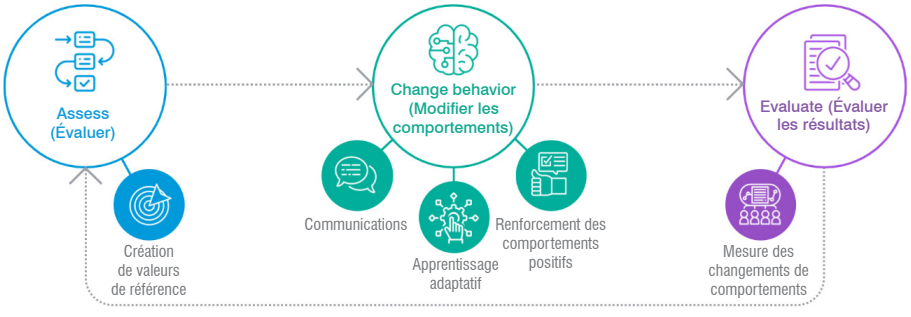

Figure 1. Le cadre Proofpoint ACE (Assess, Change behavior, Evaluate).

Cette fiche solution décrit comment Proofpoint Security Awareness Training peut vous aider à :

- Stimuler l'engagement de vos utilisateurs
- Optimiser le temps de formation limité des utilisateurs
- Renforcer les comportements positifs et améliorer l'efficacité de l'apprentissage
- Étendre et développer votre programme de sensibilisation à la sécurité informatique

Approche de l'apprentissage adaptatif

Notre approche efficace basée sur l'apprentissage adaptatif peut vous aider à motiver les utilisateurs en leur proposant une expérience d'apprentissage plus personnalisée. Elle cible en effet leurs besoins spécifiques : lacunes au niveau des connaissances, rôles, méthodes d'apprentissage et vulnérabilités. Cette section décrit chacun de ces éléments plus en détail.

Lacunes en termes de connaissances

Nos formations comportent des niveaux de difficulté différents et abordent plusieurs domaines de base et de spécialisation. Vous pouvez affecter aux utilisateurs des modules distincts en fonction de leur niveau de connaissances. La formation aborde des sujets tels que les suivants :

- Email et ingénierie sociale
- Terminaux mobiles
- Sécurité Internet et cloud
- Mots de passe et authentification
- Gestion et protection des données
- Développement logiciel sécurisé
- Opérations sécurisées
- Sécurité physique et télétravail
- Menaces internes
- Conformité

Rôles

Vous pouvez offrir des formations ciblées destinées à des groupes précis d'utilisateurs, correspondant à leur rôle dans l'entreprise. Nous proposons divers modèles et modules adaptés à différents rôles, par exemple le département financier, les RH, les collaborateurs en télétravail, le service juridique, etc. Vous pouvez rechercher la formation appropriée et la soumettre aux utilisateurs endossant ces rôles.

Méthodes d'apprentissage

Notre contenu est structuré en différentes catégories et disponible sous divers supports, avec plusieurs styles et formats — animations, vidéos en live action, vidéos humoristiques, interactions, aventures, jeux, affiches, newsletters ou prospectus. L'objectif est de vous permettre de trouver le style qui correspond le mieux à votre culture d'entreprise et à vos utilisateurs. Cette variété signifie que vous trouverez toujours un type de contenu attirant pour chaque utilisateur dans votre entreprise.

Vulnérabilités

Proofpoint dispose d'une threat intelligence riche que vous pouvez utiliser pour dispenser une formation basée sur les menaces en circulation. Lorsqu'elle est intégrée à notre plate-forme Proofpoint Threat Protection, notre solution de sensibilisation à la sécurité informatique vous offre une visibilité sur les collaborateurs qui se laissent le plus piéger et sur les VAP (Very Attacked People™, ou personnes très attaquées). Vous pouvez ensuite proposer une formation ciblée à vos VAP sur la base des menaces qu'ils sont susceptibles de rencontrer, afin de renforcer leur résilience face à celles-ci.

Threat intelligence et contenu axé sur les menaces

Notre contenu axé sur les menaces vous aide à préparer vos utilisateurs à faire face aux attaques courantes en environnement réel. Nous proposons des alertes sur les menaces opportunes centrées sur les dernières attaques en date observées chez nos clients. Nous publions aussi

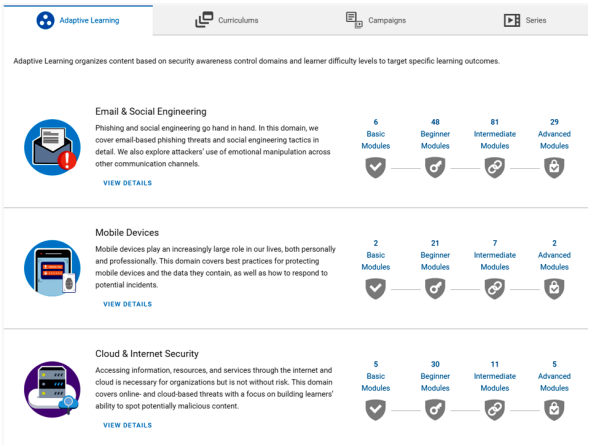

Figure 2. L'apprentissage adaptatif permet de proposer des formations correspondant à différents domaines et niveaux de difficulté, afin de cibler des utilisateurs aux lacunes différentes.

Figure 3. Proofpoint propose un large éventail de formats et de styles de formation, pour s'adapter au mieux aux besoins de vos utilisateurs.

régulièrement du contenu Attack Spotlight pour que vous puissiez améliorer vos programmes de sécurité avec des formations qui préparent les apprenants à rester vigilants dans la perspective de la prochaine attaque. Cette possibilité est offerte à tous, indépendamment d'une intégration avec Proofpoint Targeted Attack Protection (Proofpoint TAP).

Optimisation du temps de formation grâce au microapprentissage

Nous fournissons des modules de microapprentissage qui assurent que le temps consacré à la formation est utilisé de manière efficace. Un grand nombre de ces modules ont une durée de trois minutes ou moins. Chaque module est associé à des objectifs et résultats d'apprentissage clairs. Ils abordent plusieurs domaines et sujets clés pour que tous vos utilisateurs disposent de bonnes bases de sensibilisation à la sécurité informatique. Notre programme de microapprentissage de base peut être suivi en une heure environ (heure totale d'exécution).

Les utilisateurs peuvent intégrer ces exercices de formation rapides et ciblés dans leur planning journalier et les intercaler entre leurs tâches quotidiennes. Leur principal avantage est qu'ils vous offrent la flexibilité nécessaire pour élaborer des parcours de formation personnalisés pour vos utilisateurs. Vous pouvez utiliser les modules de microapprentissage pour élaborer les formations à suivre ainsi que les évaluations associées.

Proofpoint élabore et étend son offre de formation par l'intermédiaire de programmes de cours. Il s'agit de sélections de contenus spécifiquement conçues en vue de la réalisation de tâches spécifiques. Ces programmes de cours facilitent votre prise de décision lorsque vous élaborez des formations à l'intention des apprenants. Ils peuvent vous aider à former facilement les utilisateurs sur des sujets tels que des normes et cadres de sécurité très utilisés, comme NIST et ISO.

Figure 4. L'intégration avec le tableau de bord TAP procure aux administrateurs des informations pertinentes sur les collaborateurs qui se laissent le plus piéger et sur les utilisateurs vulnérables (au sein du tableau de bord). Vous pouvez ainsi élaborer un plan de formation ciblé à leur intention dans la plate-forme de sensibilisation à la sécurité informatique.

Les messages éducatifs affichent des informations contextuelles lorsque les collaborateurs tombent dans le piège de simulations de phishing. Ces messages comprennent un bref commentaire avec les raisons pour lesquelles il ne fallait pas cliquer sur le message en question, ce qui aide les utilisateurs à apprendre par l'exemple, dans un environnement sûr.

Renforcement des comportements positifs et de l'efficacité de l'apprentissage

Cette section décrit quelques-unes des façons dont Proofpoint vous aide à renforcer les comportements positifs.

Formation juste à temps

Les messages éducatifs de Proofpoint affichent des informations contextuelles lorsque les collaborateurs tombent dans le piège de simulations de phishing. Ces messages comprennent un bref commentaire avec les raisons pour lesquelles il ne fallait pas cliquer sur le message en question, ce qui aide les utilisateurs à apprendre par l'exemple, dans un environnement sûr. Nous vous proposons des modèles de messages éducatifs pour vous aider à démarrer, mais vous pouvez également les personnaliser pour répondre à vos besoins et pour les adapter aux simulations de phishing envoyées. Une telle approche vous offre davantage de contrôle sur ce que les apprenants reçoivent et voient.

Feedback utilisateur personnalisé

Lorsque les utilisateurs signalent une tentative de phishing dans le cadre d'une simulation, nous les informons qu'ils ont réussi le test de phishing. Lorsque les utilisateurs signalent un message suspect réel, vous pouvez personnaliser le feedback avec notre solution CLEAR (Closed-Loop Email Analysis and Response) et les notifier automatiquement du verdict sur l'email signalé. Ce retour les encourage à continuer à signaler les menaces potentielles. Il permet également d'entretenir une relation avec les utilisateurs.

Avertissements contextuels

Notre solution permet l'affichage d'avertissements contextuels lorsqu'elle est intégrée avec la plate-forme Proofpoint Threat Protection. Ces avertissements alertent les utilisateurs en cas d'emails suspects, pour leur rappeler la nécessité de prendre le temps d'examiner leurs messages avant d'effectuer toute action. Le bouton « Report Suspicious » (Signaler comme suspect) leur rappelle également la possibilité de signaler toute menace potentielle. Ensemble, ces fonctionnalités améliorent le taux de signalement et le taux de précision de ces signalements.

Évaluations d'apprentissage adaptatif

Proofpoint propose des évaluations d'apprentissage adaptatif. Il s'agit de tests rapides et concis qui vous permettent de suivre facilement l'évolution de la compréhension des utilisateurs par sujet. Vous pouvez mettre en correspondance une évaluation avec l'un des trois styles de modules. Toutes les évaluations sont associées aux mêmes résultats d'apprentissage et permettent d'identifier précisément ce que les utilisateurs comprennent, ainsi que ce qui leur pose des difficultés. Ces évaluations peuvent être affectées à des utilisateurs en tant que tests avant ou après apprentissage, correspondant aux modules de microapprentissage. Vous pouvez suivre les résultats en temps réel avec les détails des affectations au sein de la plate-forme.

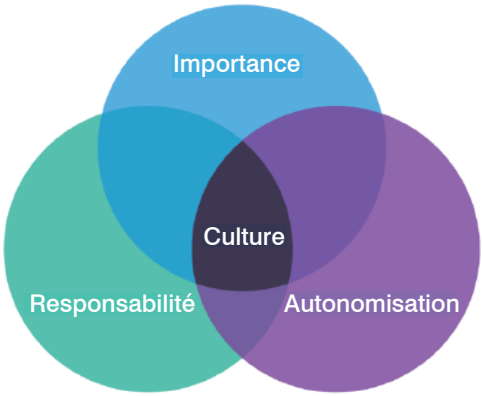

Figure 5. Facteurs concomitants contribuant à une culture de la sécurité.

Développement de votre programme de sensibilisation à la sécurité informatique

Évaluation de la culture de sécurité dans l'entreprise

Proofpoint vous permet d'étendre la portée de votre programme de formation en vous aidant à identifier les perceptions des utilisateurs. Il s'agit là d'une étape essentielle pour instaurer une culture de la sécurité forte. Selon Proofpoint, une culture de la sécurité est le recoupement entre trois dimensions :

- **Responsabilité.** Les collaborateurs se sentent-ils, individuellement et collectivement, responsables de leurs actes en faveur de la prévention des cybermenaces ?
- **Importance.** Les collaborateurs sont-ils conscients qu'une menace pourrait les toucher personnellement ?
- **Autonomisation.** Les collaborateurs se sentent-ils capables d'identifier et de signaler les comportements suspects ?

Notre évaluation de la culture d'entreprise vous aide à déterminer l'état actuel de cette dernière. Elle dresse un état des lieux des perceptions des utilisateurs en matière de cybersécurité. Elle favorise le diagnostic des changements de comportements au fil du temps et permet d'estimer la probabilité qu'un utilisateur exécute l'action appropriée. Grâce au rapport d'évaluation, vous pouvez adapter vos messages et votre formation à des groupes d'utilisateurs spécifiques, les rendant plus pertinents et efficaces.

Langues prises en charge

À l'intention des entreprises internationales, Proofpoint propose la prise en charge de plus de 40 langues dans son programme de microapprentissage de base, avec à la fois des sous-titres et du voice-over. De plus, une grande partie de nos autres modules de formation sont localisés dans au moins 11 langues. Notre fonctionnalité d'exportation multilingue SCORM vous permet de télécharger ou d'héberger facilement du contenu de formation pour un public international en quelques clics seulement. Grâce à notre large éventail de modules et vidéos de formation, nous adoptons une approche de diversité et d'inclusion dans le respect des différentes cultures et origines des utilisateurs.

Résumé

Former les utilisateurs disposant d'un temps limité et de priorités parfois conflictuelles, dans un paysage des menaces en perpétuelle évolution, nécessite une solution de sensibilisation à la sécurité informatique capable de combler efficacement les lacunes en termes de connaissances. Avec Proofpoint Security Awareness Training, vous pouvez proposer à vos utilisateurs une formation opportune et ciblée. Celle-ci les aidera à adopter des habitudes saines en matière de cybersécurité, qu'ils pourront ensuite appliquer tant sur leur lieu de travail qu'en dehors de celui-ci. Ils deviendront ainsi une ligne de défense solide pour l'entreprise et un acteur vigilant en soutien de l'équipe de sécurité.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.