

Proofpoint Essentials – Security Awareness

PRINCIPAUX AVANTAGES

- Réduction de 90 % du nombre d'attaques de phishing et d'infections de malwares
- Modification du comportements des utilisateurs
- Formations cohérentes conçues pour les PME
- Contenus traduits dans plus de 35 langues
- Suivi des résultats et des progrès des utilisateurs grâce à des rapports clairs

La solution Proofpoint Essentials – Security Awareness permet aux PME de proposer la formation appropriée aux collaborateurs concernés au moment opportun. Elle transforme vos utilisateurs finaux en véritables piliers de défense contre les cyberattaques.

Plus de 90 % des cyberattaques actuelles ciblent les utilisateurs par le biais de la messagerie électronique¹. Bien que les technologies de sécurité soient utiles pour s'en prémunir, elles ne peuvent pas contrer toutes les menaces. C'est pourquoi vous devez former vos collaborateurs afin qu'ils deviennent de véritables piliers de votre défense. Vos utilisateurs doivent être capables d'identifier et de rejeter le phishing, le piratage de la messagerie en entreprise (BEC, Business Email Compromise) et autres menaces. Un programme efficace de formation et de sensibilisation à la sécurité informatique montre à vos collaborateurs comment éviter d'ouvrir la porte aux cybercriminels.

Nous avons conçu la solution Proofpoint Essentials – Security Awareness afin de répondre aux besoins uniques des PME. Notre approche centrée sur les personnes contribue à modifier efficacement les comportements des collaborateurs. Elle vous permet de réduire l'exposition de votre entreprise aux compromissions, tout en minimisant les temps d'arrêt des collaborateurs.

PROTECTION DE L'ENTREPRISE AVEC LES SIMULATIONS DE PHISHING THREATSIM

Pour mettre en place un programme efficace de sensibilisation à la sécurité, vous devez proposer à vos utilisateurs la formation dont ils ont réellement besoin. Nos simulations d'attaques de phishing ThreatSim® évaluent la vulnérabilité de vos utilisateurs face à un large échantillon d'attaques de phishing et de spear phishing (harponnage). Vous pouvez choisir parmi des milliers de modèles répartis dans 13 catégories pour évaluer le comportement des utilisateurs face à de multiples types de menaces, notamment :

- Pièces jointes malveillantes
- URL dangereuses
- Demandes de données personnelles

Vous devez également maintenir vos formations à jour dans un paysage des menaces en constante évolution. Nous ajoutons de nouveaux modèles toutes les semaines afin qu'ils reflètent les tendances actuelles des attaques. Ces simulations d'attaques de phishing comprennent des modèles dynamiques fondés sur :

- la threat intelligence recueillie par Proofpoint ;
- les demandes des clients ;
- les tendances saisonnières.

¹ Verizon, « Data Breach Investigations Report » (Rapport d'enquête sur les compromissions de données), mai 2019.

Les utilisateurs qui tombent dans le piège reçoivent immédiatement des explications et des conseils pour préciser les objectifs de la simulation, démontrer les dangers d'une attaque réelle et apprendre comment éviter de se laisser piéger à l'avenir. Vous pouvez également assigner automatiquement une formation à ceux qui échouent lors d'une simulation de phishing.

Formation des collaborateurs avec du contenu attrayant et directement applicable

Nos contenus de formation reposent sur des principes pédagogiques à l'efficacité reconnue et couvrent un large éventail de risques de sécurité. Qui plus est, nous actualisons constamment les modules interactifs et ludiques de notre bibliothèque de contenus afin qu'ils reflètent les dernières tendances en matière d'attaques. Les messages sont cohérents et le contenu est disponible dans plus de 35 langues.

Vos utilisateurs peuvent suivre nos formations à tout moment, n'importe où et sur tout terminal connecté. Il ne faut que 5 à 15 minutes pour suivre un module complet, ce qui permet à vos utilisateurs de les suivre sans que leur travail en soit perturbé.

Nos modules interactifs sont conformes aux exigences de la section 508 et aux directives WCAG 2.0 AA (directives sur l'accessibilité des contenus Web).

Analyse des résultats grâce à des rapports complets

Nos rapports offrent une visibilité sur les vulnérabilités et les comportements de vos utilisateurs. Vous pouvez évaluer les progrès de vos collaborateurs en observant leurs interactions, leurs réactions lors des simulations d'attaques et les formations qui leur sont attribuées.

Vous trouverez des rapports dynamiques et conviviaux dans l'interface utilisateur familière de Proofpoint Essentials. Vous pouvez :

- télécharger et exporter des données ;
- partager les résultats avec d'autres parties prenantes ;
- procéder à des analyses plus détaillées ;
- comparer les indicateurs de plusieurs événements de sécurité.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : [proofpoint.com/fr](https://www.proofpoint.com/fr).

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité 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, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.