proofpoint.

PROOFPOINT PHISHING SIMULATION AND SECURITY AWARENESS

AVANTAGES CLÉS

- Corrigez le comportement des utilisateurs pour réduire les risques de phishing et de ransomware.
- Hiérarchisez et améliorez la réaction aux incidents.
- Proposez une formation uniforme à l'échelle mondiale grâce à la prise en charge multilingue.
- Suivez les résultats et la progression avec des rapports générés en temps réel.

La solution de simulation de phishing et de sensibilisation à la sécurité, Proofpoint Phishing Simulation and Security Awareness, vous aide à tester et éduquer vos employés sur les tactiques d'attaque de la messagerie. Elle vous fournit une couche de protection supplémentaire pour :

- Augmenter la prise de conscience
- Réduire le nombre d'attaques réussies par phishing et infections de malware
- Prévenir les futures failles de sécurité

Plus de 90 % des cyberattaques commencent par un e-mail. Protéger vos employés et vos données est donc crucial. Les services capables de détecter et de bloquer les e-mails malveillants sont une partie de la solution. Vous pouvez également réduire la probabilité d'attaques réussies, phishing ou ransomware, grâce à une simulation efficace des menaces et une formation de sensibilisation à la sécurité.

PROTÉGER VOTRE ORGANISATION AVEC THREATSIM PHISHING SIMULATIONS

Identifiez les employés susceptibles de devenir victimes d'attaques de phishing et de les propager grâce à ThreatSim® Phishing Simulations. ThreatSim permet aux équipes de sécurité de simuler des attaques de phishing. Cette solution vous dote de plus de 500 modèles de phishing différents, en 30 langues et 13 catégories. Elle vous permet d'évaluer la réaction des utilisateurs face à de multiples menaces, dont :

- Les pièces jointes malveillantes
- Les liens incorporés
- Les demandes de données personnelles
- Et bien d'autres...

Nous ajoutons chaque mois de nouveaux modèles basés sur les demandes des clients, les sujets d'actualité et les véritables e-mails de phishing observés dans la pratique.

Les utilisateurs qui échouent aux simulations d'attaque reçoivent alors un enseignement pratique « au moment opportun ». Ils y découvrent l'objectif de la manœuvre et les dangers des véritables attaques, et apprennent à ne plus tomber dans le piège. Pour venir épauler vos utilisateurs les plus vulnérables, vous pouvez automatiquement affecter une formation interactive à tous ceux qui échouent lors de la simulation ThreatSim.

SENSIBILISER VOS EMPLOYÉS AVEC DES MODULES DE FORMATION INTERACTIFS

30 modules de formation interactifs sont disponibles en plus de 30 langues. Une combinaison de modules, ludiques et scénarisés, permet à vos utilisateurs de mettre leurs connaissances en pratique et d'éviter une vaste gamme d'attaques de phishing et d'escroqueries sur les réseaux sociaux. Personnalisables, nos Manuels de formation vous permettent d'ajouter du contenu au début et à la fin de chaque module.

Ces formations sont disponibles à la demande. Pour ne pas perturber l'activité quotidienne, chaque module dure en moyenne 5 à 15 minutes.

RÉDUIRE LES RISQUES AVEC PHISHALARM ET PHISHALARM ANALYZER

PhishAlarm® intègre la prévention du phishing au poste de travail. Le complément PhishAlarm pour le client de messagerie étant inclus dans ThreatSim, un simple clic permet à votre personnel de signaler les messages suspects. L'utilisateur qui signale un e-mail est aussitôt conforté par un message contextuel ou un e-mail de remerciement.

PhishAlarm Analyzer établit la priorité des messages signalés et améliore la réaction aux incidents. Il permet aux administrateurs de rapidement examiner les principaux détails, prendre une décision et agir. Avec Phish Alarm et PhishAlarm Analyzer, vous êtes à même de réduire les risques inhérents aux attaques de phishing qui sévissent actuellement.

ÉVALUER VOS LACUNES AVEC CYBERSTRENGTH

Cyberstrength® est un puissant outil d'évaluation Web capable d'identifier les secteurs dans lesquels vos employés sont susceptibles d'être vulnérables, sans passer par une fausse attaque. Cyberstrength évalue les connaissances de vos employés sur les principales questions liées à la cybersécurité pour établir une référence de base. Cette référence vous permet ensuite de réévaluer régulièrement leurs connaissances pour suivre leur progression et corriger les secteurs préoccupants.

Notre bibliothèque comprend plus de 175 questions. Vous pouvez également créer vos propres questions afin de vérifier si votre personnel connaît bien les politiques et les procédures de votre organisation. Cyberstrength vous permet d'identifier les secteurs vulnérables, au niveau de l'organisation comme des individus.

Disponibles en différentes combinaisons adaptées aux besoins des clients, nos offres de simulation et sensibilisation à la sécurité améliorent votre profil vis-à-vis des risques en testant et en formant vos employés.

Fonctionnalités	Anti-Phishing	Foundations	Enterprise
ThreatSim	✔	✔	✔
PhishAlarm	✔	✔	✔
PhishAlarm Analyzer			✔
CyberStrength		✔	✔
Nombre de modules de formation	3	12	Tous

À PROPOS DE PROOFPOINT
Proofpoint Inc. (NASDAQ:PFPT), leader spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger leurs données contre les menaces avancées, et de se conformer aux réglementations en vigueur. Grâce à Proofpoint, les professionnels de la cybersécurité sont en mesure d'accéder à des renseignements et outils capables de protéger les utilisateurs et leurs données contre les attaques menées par courrier électronique, sur les réseaux sociaux ou les appareils mobiles. De nombreuses entreprises de toutes tailles, dont plus de la moitié de celles figurant dans le classement Fortune 100, exploitent des solutions Proofpoint. Celles-ci sont conçues spécialement pour les environnements mobiles et de réseaux sociaux. Elles tirent parti de la puissance du cloud et d'une plateforme d'analyse pilotée par les Big Data pour lutter contre les menaces avancées modernes.

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques contenues dans le présent document sont la propriété de leurs détenteurs respectifs.