proofpoint.

SUITE PROOFPOINT DE FORMATION À LA LUTTE CONTRE LE PHISHING

PRINCIPAUX AVANTAGES

- Réduisez les risques posés par les attaques de phishing et de ransomwares grâce à un changement de comportement des utilisateurs finaux.
- Hiérarchisez et améliorez les interventions sur incident.
- Offrez des formations cohérentes dans plusieurs langues, partout dans le monde.
- Suivez les résultats et les progrès grâce à des rapports en temps réel.

Les responsables de la sécurité informatique et leurs équipes ne sont que trop conscients des défis que pose la réduction des attaques de phishing et de ransomwares. Les dispositifs techniques de protection ne permettent pas d'empêcher toutes les attaques d'atteindre les utilisateurs finaux. Ils sont notamment impuissants face aux erreurs humaines. De plus, ils sont incapables d'offrir les avantages à long terme d'une formation efficace de sensibilisation à la sécurité.

La formation continue donne des résultats mesurables. Notre suite de formation à la lutte contre le phishing, qui combine évaluation, formation, renforcement et mesure, peut être utilisée en association avec notre méthodologie de formation continue, dont l'efficacité n'est plus à démontrer. Elle constitue la solution idéale si votre objectif premier est de permettre à vos utilisateurs finaux de se défendre contre les attaques de phishing.

SIMULATIONS D'ATTAQUES DE PHISHING THREATSIM

Les simulations d'attaques de phishing ThreatSim® vous aident à prendre la mesure de la vulnérabilité de votre entreprise face à un large échantillon d'attaques de phishing et de spear phishing (harponnage). Vous pouvez choisir parmi des milliers de modèles de phishing répartis dans 13 catégories pour évaluer le comportement des utilisateurs face à de multiples types de menaces, notamment :

- Pièces jointes malveillantes
- Liens intégrés
- Demandes de données personnelles

Nous ajoutons très régulièrement de nouveaux modèles. Ces simulations d'attaques de phishing comprennent des modèles dynamiques, fondés sur les renseignements recueillis par Proofpoint, ainsi que d'autres modèles inspirés des demandes de nos clients ou axés sur des thèmes saisonniers.

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 tomber dans le piège à l'avenir. Vous pouvez également aider les utilisateurs les plus vulnérables en assignant automatiquement une formation interactive à ceux qui échouent lors d'une simulation de phishing.

MODULES DE FORMATION INTERACTIFS

Grâce à nos modules de formation interactifs, les utilisateurs peuvent s'exercer à identifier et déjouer les attaques de phishing et autres escroqueries d'ingénierie sociale. Nous proposons un éventail de modules basés sur des scénarios et sous forme de jeux. Vous pouvez également personnaliser les contenus au début et à la fin de chaque module.

Les modules de formation sont proposés dans un format adapté aux appareils mobiles et sont disponibles sur demande. Ils sont conformes aux exigences de la section 508 et aux directives internationales WCAG 2.0 AA (directives d'accessibilité des contenus Web). En moyenne, un module dure de 5 à 15 minutes.

La suite de formation à la lutte contre le phishing comprend huit de ces modules de formation :

Formation	Description
Sécurité de la messagerie	Apprend aux utilisateurs à identifier et à déjouer les menaces suivantes : • Messages de manipulation • Liens malveillants et déguisés • Pièces jointes dangereuses • Demandes de données inappropriées
Anti-Phishing Phil	Module sous forme de jeu qui apprend aux utilisateurs à détecter les attaques de phishing en identifiant les URL frauduleuses.
Anti-Phishing Phyllis	Module sous forme de jeu qui apprend aux utilisateurs à reconnaître les emails de phishing en identifiant les pièges.
Protection de la messagerie électronique – Notions fondamentales	Formation courte mais utile ciblant les risques spécifiques auxquels les utilisateurs de la messagerie électronique sont exposés. Elle comprend les quatre mini-modules suivants : • Introduction au phishing • Identification des liens dangereux • Identification des pièces jointes dangereuses • Phishing et saisie de données
Protection de la messagerie électronique – Notions avancées	Complète les connaissances acquises lors de la formation Protection de la messagerie électronique – Notions fondamentales grâce à trois modules extrêmement ciblés sur les menaces sophistiquées véhiculées par la messagerie : • Outils de protection des emails • Protection des emails sur les appareils mobiles • Attaques de spear phishing
Protection contre les ransomwares	Fournit une formation brève mais complète sur la façon de reconnaître et d'éviter les attaques de ransomwares. Les bonnes pratiques enseignées aux utilisateurs s'appliquent également à d'autres menaces, dont le phishing et les malwares.
Ingénierie sociale	Va au-delà du phishing pour expliquer les dangers associés aux attaques de SMiShing et de vishing, via les réseaux sociaux et en personne. Les utilisateurs apprennent également à détecter les techniques et pièges d'ingénierie sociale les plus courants.
Formation en matière d'URL	Examine la structure d'une URL et les signes révélateurs d'une URL suspecte, et explique comment identifier et éviter les liens malveillants.

PHISHALARM ET PHISHALARM ANALYZER (MODULES COMPLÉMENTAIRES OPTIONNELS)

PhishAlarm® est un module d'extension du client de messagerie qui permet à vos employés de signaler des emails suspects d'un simple clic. Pour renforcer immédiatement les comportements positifs, un remerciement est envoyé par message contextuel ou par email aux utilisateurs qui signalent de tels messages. Complément idéal de PhishAlarm, PhishAlarm® Analyzer hiérarchise les emails signalés et améliore les interventions sur incident en permettant aux administrateurs d'analyser rapidement les données les plus importantes pour prendre la bonne décision et agir promptement. Collectivement, ces modules limitent les risques associés aux attaques de phishing actives.

VEILLE STRATÉGIQUE QUANT AUX RISQUES POSÉS PAR LES UTILISATEURS FINAUX

Mesurez et analysez vos résultats. Nous mettons à votre disposition un éventail de rapports détaillés qui fournissent des informations globales et granulaires sur les résultats de vos mesures d'évaluation et de formation. En tant qu'administrateur, vous bénéficiez d'une visibilité étendue sur les principaux contrevenants et les récidivistes, ainsi que sur les éléments de formation les plus efficaces. Cette analyse vous aidera à mettre en place un système de défense efficace et à cibler les vulnérabilités.

À PROPOS DE PROOFPOINT, INC.

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.