Cofense PhishMe™

ENCOURAGER LES EMPLOYÉS À MIEUX RÉSISTER AUX ATTAQUES PAR PHISHING

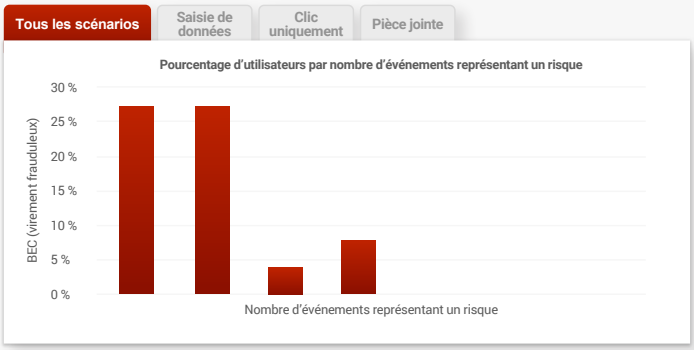
Les recherches effectuées par Cofense ont montré que les rançongiciels ont représenté plus de 97 % des courriels de phishing en 2016. Face à des chiffres aussi alarmants, que faites-vous pour protéger votre entreprise des cyberattaques ? Cofense PhishMe fait de vos employés votre ultime ligne de défense, en s'appuyant sur des méthodes éprouvées pour les encourager à adopter les comportements qui les aideront à repérer et à combattre les tentatives de phishing malveillantes , l'objectif étant que votre point le plus faible devienne votre meilleure défense.

Pourquoi choisir Cofense PhishMe™ ?

PhishMe a démontré sa capacité à réduire le risque que les employés soient victimes de cyberattaques de 95 %, préparant ainsi votre ligne de défense ultime pour repérer les tentatives de phishing les plus subtiles et y faire face.

Principaux avantages

- **Réduit de plus de 95 % la vulnérabilité de l'entreprise aux attaques de phishing via des exercices de formation**
- **Simule les tactiques d'attaque les plus récentes avec des modèles de scénario et de formation personnalisables**
- **Utilise des techniques d'apprentissage différenciées, provenant d'une bibliothèque continue de contenu multilingue**
- **Valide l'efficacité du programme et identifie les zones de risque grâce à des rapports détaillés**



En quoi consiste Cofense PhishMe™ ?

PhishMe est une plate-forme SaaS spécialisée qui permet au personnel de mieux faire face aux attaques de phishing et lui fournit des renseignements en temps réel sur les menaces en lui offrant une expérience de harponnage réaliste. Les scénarios personnalisables de la solution imitent les menaces les plus pertinentes et fournissent immédiatement un retour d'information et des conseils aux individus qui tombent dans le piège.

Notre technologie brevetée offre un éventail inégalé de scénarios de cyberattaques, de contenus et de personnalisation, mais aussi, dans chaque cas, une analyse et des rapports détaillés. L'assistance client exceptionnelle de PhishMe garantit des exercices parfaitement contrôlés, qui ne remettent pas en cause votre sécurité ni n'entraînent de conséquence négative.

Mode de fonctionnement

> Les analyses poussées de Cofense sont très précieuses. Ces données nous ont aidés à modifier nos programmes de lutte contre le phishing en ciblant davantage les formations, notamment pour les employés qui ont l'habitude de cliquer fréquemment sur les liens, afin de leur faire perdre cette habitude.
>
> **Jim Stewart, CISO, United Community Bank**

Un contenu personnalisable et une formation adaptée

Les scénarios de PhishMe peuvent être personnalisés pour simuler différentes techniques d'attaque, notamment les attaques par téléchargement furtif, programme malveillant et ingénierie sociale, ainsi que les tactiques plus élaborées comme le phishing interactif et le spear phishing (harponnage) hautement personnalisé. Les clients peuvent par ailleurs exécuter des scénarios pour étudier leur progrès par rapport au nombre croissant de clients de Cofense.

Les clients peuvent créer leurs propres scénarios ou utiliser l'un des nombreux modèles prédéfinis personnalisables. Notre bibliothèque de contenu en constante expansion couvre une multitude de sujets relatifs à la sécurité, tels que le phishing, la sensibilisation à la sécurité, la conformité et les réseaux sociaux, sous divers formats, notamment des modèles HTML5, des vidéos et un module de jeu. Avec son contenu et sa formation multilingues, Cofense répond aux différentes spécificités culturelles des entreprises locales et internationales.

Pour les organisations exigeant une formation plus poussée, Cofense propose des contenus didactiques entièrement conformes aux normes SCORM sur des sujets de sécurité générale. Les formations disponibles abordent les domaines suivants :

- **Sensibilisation au spear phishing (harponnage)**
- **Liens malveillants**
- **Programmes malveillants**
- **Sécurité des mots de passe**
- **Protection des données**
- **Appareils mobiles**
- **Sécurité de la navigation Internet**
- **Ingénierie sociale**
- **Réseaux sociaux**
- **Sécurité physique**
- **Travail en dehors du bureau**
- **Signalement des activités suspectes**
- **Rançongiciels**
- **Compromission de la messagerie d'entreprise (BEC)**
- **Harponnage avancé**

Une plate-forme de formation sécurisée

Notre plate-forme SaaS est déployée sur un site certifié Tier III SOC 2 et SOC 3 aux États-Unis et sur un site certifié ISO 9001:2008 en Europe. Ces deux sites sont testés en externe et incluent des contrôles d'accès robustes. Toutes les données sont chiffrées une fois les opérations terminées et Cofense ne collecte jamais de données sensibles sur ses clients lors des scénarios impliquant la saisie de données.

Une analyse détaillée

Chaque scénario fournit des mesures pour suivre de nombreux points de données qui, lorsqu'ils sont analysés dans le temps, offrent des informations sur la vulnérabilité de l'entreprise et un outil d'amélioration continue.

Les rapports de PhishMe suivent, par exemple, les données suivantes :

- **Géolocalisation**
- **Horodatages**
- **Réponses individuelles**
- **Tendances**
- **Temps consacré à la formation**
- **Temps écoulé jusqu'au premier rapport (Reporter requis)**
- **Énumération du navigateur**
- **Résilience organisationnelle (Reporter requis)**

Assurer la réussite du client

Chaque licence PhishMe inclut l'accès à l'assistance client exceptionnelle de Cofense. En plus de garantir l'acheminement correct des scénarios à base d'e-mail, notre équipe d'assistance propose des conseils d'expert pour mettre en œuvre PhishMe, étudier les scénarios d'e-mail par rapport aux bonnes pratiques du secteur, personnaliser le programme en fonction de la culture, de la gestion et des utilisateurs de l'entreprise, et fournir une assistance concernant les nouvelles fonctions et les nouveaux scénarios.

Si leurs ressources sont limitées, les entreprises peuvent également utiliser PhishMe en tant que solution partiellement ou entièrement gérée, avec un professionnel affecté à leur compte qui crée, exécute et analyse les résultats des campagnes. Les programmes sont personnalisés selon les besoins et la culture de l'entreprise.

Cofense™, anciennement PhishMe®, est le leader mondial, dirigée par l'être humain, de solutions de défense contre le Phishing des entreprises qui craignent d'être compromises par des cyberattaques sophistiquées. Cofense met en œuvre une démarche collaborative en matière de cybersécurité en permettant à l'ensemble de votre organisation de réagir face au vecteur d'attaque le plus courant : le Phishing. Cofense répond aux besoins d'organisations diverses de toutes tailles, notamment dans les secteurs des services financiers, de l'énergie, de l'administration, de la santé, de la technologie, de la production et bien d'autres encore, figurant parmi les 1000 sociétés les plus grandes du monde. Ces entreprises perçoivent l'impact considérable du changement des comportements des utilisateurs pour améliorer la sécurité, réagir rapidement aux incidents et réduire le danger de pénétration

COFENSE

Pour en savoir plus, contactez :

Site Web : cofense.com/contact Tél. : 703 652 0717
Adresse : 1608 Village Market Blvd, SE #200
Leesburg, VA 20175, États-Unis