**Communiqué de presse**

*41% des entreprises sont exposées à une cyberattaque quotidiennement; 62% des entreprises ne forment pas leurs employés à détecter les tentatives de phishing*

**Sophos lance Phish Threat, un outil de simulation d’attaques de phishing accompagné de modules de formation avec un support multilingue**

* *Facilite l'intégration d’une formation de sensibilisation aux emails au sein d’une stratégie globale de sécurité.*
* *Offre un meilleur retour sur investissement et des mesures de risque améliorées, avec un reporting centralisé et un suivi des données analysées.*

Bruxelles, 13 mars 2018 - **Sophos annonce aujourd'hui l'extension de son simulateur d'attaques de phishing Sophos Phish Threat, accompagné de ses modules de formation, en Europe et en Asie. Avec des tableaux de bord améliorés et de nouvelles capacités d’analyse pour suivre les risques organisationnels et les performances des employés, Phish Threat simplifie un élément clé de la stratégie cybersécurité d'une entreprise : la sensibilisation et la formation des employés. Grâce à la possibilité de choisir parmi des sites d'hébergement en Allemagne, en Irlande ou aux États-Unis, les entreprises du monde entier peuvent désormais accéder à une formation cybersécurité interactive et multilingue, à partir de Sophos Central, la plateforme de gestion de la sécurité de Sophos.**

Le phishing est une technique simple mais redoutablement efficace pour diffuser les charges actives des ransomwares et pour voler des données. Avec 41%[[1]](#footnote-1) des entreprises exposées à une cyberattaque quotidiennement, la formation des employés est cruciale pour maintenir un niveau de sécurité efficace. Sophos Phish Threat automatise l'ensemble du processus de formation et fournit des analyses visuelles pour rapidement identifier et aider les employés les plus vulnérables à mieux se protéger. C’est le seul outil de sensibilisation et de formation à la cybersécurité à être complètement intégré dans l’offre de protection d’un leader du secteur, ce qui le rend accessible à un large public d’entreprises, capables ainsi de gérer conjointement la sécurité de leur messagerie électronique, de leurs systèmes Endpoint et de leurs réseaux à partir d’une console unique, pour améliorer la gestion des risques et la réactivité vis-à-vis des incidents.

« Le comportement humain est un élément critique de la cybersécurité. Cependant, 62% des entreprises ne forment pas leurs employés à détecter les tentatives de phishing », déclare Bill Lucchini, Senior Vice President et General Manager de Sophos Messaging Security Group . « Les SophosLabs détectent des malwares dans 77% des emails bloqués. La création d’une véritable culture de sensibilisation en matière de cybersécurité et de protection des données est devenue une priorité absolue, étant donné le risque accru de propagation de ransomwares par email et l'introduction prévue d'une nouvelle législation telle que le RGPD. Les employés doivent être responsables de la manière avec laquelle ils traitent les données, et la capacité à repérer une attaque de phishing doit faire partie de leur formation. Sophos Phish Threat sensibilise les employés en permettant de simuler des attaques de phishing selon des techniques classiques ayant prouvé leur efficacité, ainsi qu’en utilisant d’autres exemples plus récents et innovants. Ainsi, après une campagne de sensibilisation constituée de quatre simulations Phish Threat par email, les entreprises ont constaté en moyenne une réduction de 31%[[2]](#footnote-2) de la vulnérabilité des employés ».

Phish Threat permet aux responsables informatiques d'identifier les employés vulnérables et de gérer des simulations pertinentes par emails de phishing, afin de proposer des sessions de formation plus efficaces à partir de Sophos Central. Les modèles d'attaque et les modules de formation sont disponibles en neuf langues et sont constamment mis à jour par Sophos en fonction de l’évolution du paysage des cybermenaces. Lorsque des erreurs sont commises, les employés reçoivent automatiquement une formation corrective pour mieux comprendre leurs erreurs. Phish Threat fournit également des analyses statistiques et une synthèse d’indicateurs, permettant le suivi et la mesure du risque global et comportemental en matière de cybersécurité, d’un point de vue collectif et individuel. Avec des données de référence disponibles concernant la vulnérabilité des employés vis-à-vis du phishing et en adéquation avec les normes internationales, la formation peut être entièrement personnalisée. Les données peuvent être ainsi utilisées pour améliorer la stratégie de sécurité au sein de Sophos Central, afin de fournir une stratégie de sécurité multi-niveaux vis à vis d’attaques de phishing et par ingénierie sociale.

Découvrez les dernières actualités sécurité et nos commentaires sur notre blog, déjà récompensé, Naked Security News, et pour en savoir plus sur Sophos, visitez sur notre blog sécurité.

Protégez chaque Mac et PC à votre domicile avec [Sophos Home](https://www.sophos.com/lp/sophos-home.aspx), le logiciel de cybersécurité dernière génération, à la gestion centralisée, gratuit et en ligne.

**Connectez-vous à Sophos où que vous soyez via** : [Twitter](http://twitter.com/sophos), [LinkedIn](http://soph.so/Cfv36), [Facebook](http://soph.so/CfvaA), [Spiceworks](http://soph.so/Cgbwa%20), [YouTube](http://www.youtube.com/user/sophoslabs), [Google+](https://plus.google.com/+sophos)

**Au sujet de Sophos**Sophos est un leader dans la sécurité des réseaux et des systèmes Endpoint Next-Generation et, en tant que pionnier en matière de sécurité synchronisée, développe une offre innovante qui comprend des solutions pour le chiffrement, les systèmes Endpoint, le web, les emails, les mobiles et les réseaux, capables de toujours mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 30 000 partenaires agreés. Le siège social de Sophos se situe à Oxford (Royaume-Uni), et Sophos est coté à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Informations presse:**

Sandra Van Hauwaert, Square Egg, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816

1. Freeform Dynamics, Phishing Temperature Check Report, 2017 [↑](#footnote-ref-1)
2. Données calculées à partir d’un échantillon de 10 000 campagnes récentes d’attaques de Phishing [↑](#footnote-ref-2)