

# PhishER PLUS

## Renforcez votre défense contre l'hameçonnage avec PhishER Plus

### Principaux avantages

- L'intégration complète au Phish Alert Button de KnowBe4 permet une priorisation automatique des e-mails qui ne constituent pas une menace.
- Filtrez les messages de votre boîte de réception de réaction aux incidents et traitez plus rapidement et efficacement les menaces les plus graves.
- Libérez du temps et des ressources pour vos équipes de réponse aux incidents afin d'identifier et gérer les 90 % de messages qui sont soit du courrier indésirable, soit des e-mails légitimes, en réduisant le volume d'e-mails que votre centre des opérations de sécurité doit assainir.
- Bloquez les menaces par e-mail qui ont pu contourner tous les autres filtres ou systèmes de sécurité des e-mails avant qu'elles n'atteignent les boîtes de réception de vos utilisateurs.
- Isolez les e-mails malveillants qui ont déjà contourné vos filtres grâce à la quarantaine automatique de PhishRIP Global.
- Mutualisez la veille sur les menaces grâce à plus de 10 millions d'utilisateurs formés par KnowBe4.
- Exploitez la puissance des informations sur les menaces triplement validées afin de protéger votre organisation de nouvelles attaques.
- Analysez des agrégats ou des groupes de messages en fonction de schémas récurrents pour vous aider à identifier une attaque par hameçonnage d'envergure contre votre organisation.
- Des modèles d'e-mails automatisés vous permettent d'apporter rapidement à vos employés la réponse dont ils ont besoin pour continuer à travailler.
- Créez des flux de travail personnalisés pour réaliser les tâches telles que la priorisation et l'émission d'alertes, afin que l'équipe de réaction aux incidents puisse se concentrer sur les messages pertinents.

D'année en année, les menaces par e-mail deviennent de plus en plus élaborées. Un pourcentage inquiétant de celles-ci parvient à franchir votre passerelle de messagerie sécurisée et se retrouve dans les boîtes de réception de vos utilisateurs. Les attaques d'ingénierie sociale visent de plus en plus vos utilisateurs les plus à risque. Le « Data Breach Investigation Report 2023 » de Verizon montre qu'à eux seuls, les e-mails sont la cause principale de violations de données. Récemment, des chercheurs d'ArmorBlox ont signalé que 56 % des attaques contournent vos filtres de sécurité hérités. Résultat ? Les différents systèmes de sécurité des e-mails hérités ne bloquent pas ces bombes à retardement numériques et leur permettent de s'infiltrer dans les boîtes de réception de vos utilisateurs.

### Une défense préventive et révolutionnaire contre l'hameçonnage

PhishER Plus est la protection contre l'hameçonnage la plus puissante au monde. PhishER Plus est alimenté par un flux de menaces global unique de KnowBe4. Ce flux de menaces d'hameçonnage triplement validé bloque automatiquement les attaques par hameçonnage *avant* qu'elles n'atteignent les boîtes de réception de vos utilisateurs, grâce :

1. au réseau mondial KnowBe4, qui compte plus de 10 millions d'utilisateurs finaux ayant reçu une formation de pointe, ainsi que leurs administrateurs PhishER ;
2. à PhishML, une intelligence artificielle unique entraînée à détecter les e-mails d'hameçonnage que les autres filtres n'ont pas repérés ;
3. aux informations sur les menaces traitées par des êtres humains au sein du laboratoire d'identification des menaces KnowBe4.

KnowBe4 voit ce que personne d'autre n'arrive à voir. Les utilisateurs signalent l'ensemble des attaques qui passent au travers de tous les autres filtres disponibles. Ces menaces en circulation constituent les attaques d'ingénierie sociale les plus dangereuses à un moment donné.

### Fonctionnement de PhishER Plus

PhishER Plus a été développé pour vous aider à renforcer les défenses et la sécurité des e-mails de votre organisation. Il s'agit d'une barrière supplémentaire après l'échec de votre passerelle de messagerie sécurisée actuelle et des autres systèmes de cybersécurité.

PhishER Plus active un flux de travail essentiel pour aider vos équipes de réponse aux incidents à collaborer afin d'atténuer la menace d'hameçonnage. C'est l'outil idéal pour les organisations qui souhaitent prioriser et gérer automatiquement les messages potentiellement malveillants, de manière efficace et rapide ! PhishER Plus est disponible en tant que produit indépendant ou option d'extension pour les clients KnowBe4.



# Fonctionnement de PhishER Plus



## Priorisation automatique des messages

PhishER Plus vous permet de définir le niveau de priorité de chaque message signalé selon trois catégories : Légitime, Courrier indésirable ou Menace. Les règles YARA vous permettent d'attribuer vos tâches les plus importantes, et PhishER Plus vous aide à développer un processus qui priorise automatiquement autant de messages que possible sans intervention humaine. PhishER Plus permet à votre équipe de traiter plus rapidement les menaces les plus dangereuses en examinant les attributs des messages signalés et en classant les messages les plus critiques en fonction du degré de gravité.

## Salles d'urgence

Des « salles d'urgence » vous aident à identifier les messages similaires signalés par vos utilisateurs. PhishER Plus regroupe ces messages selon leurs points communs et les présente dans un affichage préfiltré par le système en fonction des objets, expéditeurs, pièces jointes et URL clés. Chaque salle d'urgence est interactive, ce qui vous permet d'explorer de manière hiérarchique les affichages préfiltrés de la boîte de réception et de prendre les mesures nécessaires pour tous les messages correspondants.

## Intégrations

Grâce à l'intégration de l'API de PhishER Plus et à la prise en charge de plusieurs destinations syslog, vous pouvez connecter PhishER Plus aux produits de votre système de sécurité actuel et transférer ainsi les données vers les plateformes populaires de sécurité des e-mails, de veille sur les menaces, de création de tickets et de gestion des informations et des événements de sécurité. Vous pouvez également envoyer des événements à partir de PhishER Plus et les ajouter à la chronologie de vos utilisateurs dans votre plateforme KnowBe4. Vous pouvez utiliser ces événements pour créer des campagnes d'hameçonnage et de formation spécifiques permettant à vos utilisateurs de mieux identifier et signaler les e-mails suspects grâce au Phish Alert Button. PhishER Plus s'intègre également à des services externes tels que VirusTotal, pour faciliter l'analyse des pièces jointes et des domaines malveillants.

## Veille sur les menaces validées par des êtres humains

L'union fait la force. Exploitez la puissance du laboratoire d'identification des menaces KnowBe4 et du réseau d'utilisateurs finaux mondial KnowBe4 pour vous protéger contre les tentatives d'hameçonnage et les attaques d'ingénierie sociale de plus en plus élaborées.

## Liste de blocage globale de Microsoft 365

La fonctionnalité de liste de blocage globale de PhishER Plus vous permet de créer facilement une liste unique d'entrées pour la liste de blocage de votre organisation, améliorant ainsi considérablement vos filtres d'e-mails Microsoft 365, sans devoir quitter la console PhishER Plus. Les entrées de la liste de blocage concernant des menaces avérées recueillies auprès de plus de 10 millions d'utilisateurs formés sont exploitées pour empêcher automatiquement les messages correspondants d'atteindre les boîtes de réception de vos utilisateurs.

Ce flux de menaces est mis à jour en permanence et géré par KnowBe4. Il peut être synchronisé avec votre serveur de messagerie Microsoft 365. Vous pouvez également utiliser votre propre liste de blocage privée pour Microsoft 365 à la place de la liste globale.

## PhishML™

PhishML est un module d'apprentissage automatique de PhishER Plus qui vous permet d'identifier et d'évaluer les messages suspects signalés par vos utilisateurs, au début de votre processus de priorisation des messages. PhishML analyse chaque message arrivant sur la plateforme PhishER Plus et vous fournit les informations nécessaires afin de rendre le processus de priorisation plus facile, rapide et précis.

PhishML apprend en permanence à partir des messages qui sont signalés, que ce soit par vous ou par les autres membres de la communauté d'utilisateurs PhishER Plus ! Cela signifie que le modèle d'apprentissage est alimenté par de nouvelles données afin d'améliorer en permanence sa précision. Davantage de messages peuvent être priorisés automatiquement en fonction de la catégorisation PhishER Plus afin de vous faire gagner encore plus de temps.

## PhishRIP Global™

PhishRIP Global est une fonction de mise en quarantaine des e-mails qui s'intègre à Microsoft 365 et à Google Workspace afin que votre équipe de réaction aux incidents puisse agir rapidement et facilement.

PhishRIP Global vous permet de supprimer une menace identifiée de toutes les boîtes de réception des utilisateurs, d'immuniser ces boîtes de réception contre les menaces non signalées, et de vous protéger contre de futures menaces en supprimant et en mettant en quarantaine certains e-mails ou en restaurant des e-mails légitimes. Les messages qui correspondent à des menaces d'hameçonnage identifiées que d'autres clients PhishER Plus ont éliminées des boîtes de réception de leur organisation sont validés par le laboratoire d'identification des menaces KnowBe4. Ces messages sont automatiquement mis en quarantaine et supprimés des boîtes de réception de vos utilisateurs.

## PhishFlip™

PhishFlip est une fonctionnalité de PhishER Plus qui transforme automatiquement les attaques par hameçonnage ciblant votre organisation et signalées par vos utilisateurs en campagnes sécurisées de simulation d'hameçonnage sur votre plateforme KnowBe4. Avec PhishFlip, vous pouvez immédiatement transformer une attaque dangereuse en opportunité de formation concrète pour vos utilisateurs.

## Intégration de CrowdStrike Falcon Sandbox

Cette intégration permet aux administrateurs disposant d'une licence CrowdStrike Falcon Sandbox d'enquêter plus rapidement et plus efficacement sur des fichiers potentiellement malveillants depuis une seule et même console. CrowdStrike Falcon Sandbox est un outil de détection des programmes malveillants qui permet d'analyser en toute sécurité des fichiers et des URL à la recherche de contenu malveillant depuis un environnement protégé et isolé.

PhishER Plus intègre des données mutualisées d'intelligence humaine validées par l'IA, recueillies auprès des utilisateurs les mieux formés et aux parcours les plus variés sur le plan technique du monde entier. Les clients de KnowBe4 représentent au total plus de 65 000 organisations et plus de 55 millions d'utilisateurs. **C'est simple. L'union fait la force.**