opentext™ | Cybersecurity

DATASHEET

Webroot® Formation à la sensibilisation à la sécurité

Réduire l'exposition aux risques via les utilisateurs internes

Le phishing est une pratique très répandue parmi les pirates informatiques, car il s'agit d'une attaque qui peut être aisément déployée et 74 % de ces tentatives visant des entreprises américaines sont couronnées de succès.[1] Quelle que soit la taille d'une entreprise, celle-ci constitue une cible pour les cybercriminels. En effet, il suffit d'un seul clic involontaire sur un lien de phishing pour permettre aux criminels d'accéder à toutes les données stockées sur un réseau donné, voire plus. C'est également la raison pour laquelle les formations de sensibilisation à la sécurité et les simulations de phishing sont essentielles pour les entreprises qui souhaitent faire passer les utilisateurs finaux du statut de maillon le plus faible de la chaîne de sécurité à celui de première ligne de cyberdéfense véritablement résiliente.

La meilleure sécurité au monde ne peut empêcher un employé, travaillant sur site ou à distance, de laisser accidentellement la porte d'entrée du réseau grande ouverte. La formation Webroot® Security Awareness Training aide les entreprises à donner aux utilisateurs finaux les moyens d'identifier et de signaler les escroqueries, d'éviter les risques, de satisfaire aux exigences de conformité réglementaire et de contribuer à prévenir les cyberattaques modernes grâce à des formations régulières dans le cadre de l'approche de défense par couches afin de devenir cyberrésilient.

Réduire les risques avec une formation de sensibilisation à la sécurité

Suivre l'évolution des menaces et des nouveaux vecteurs d'attaque

La formation Webroot® Security Awareness Training propose une formation et des tests continus, pertinents et mesurables, nécessaires aux entreprises pour minimiser les comportements à risque des utilisateurs et atteindre la cyber-résilience. Le simulateur de phishing complet propose une bibliothèque de modèles, qui ne cesse de s'étoffer et qui se base sur des scénarios concrets. Les modèles sont catégorisés et régionalisés pour faciliter leur utilisation, tandis que la randomisation du calendrier permet une diffusion échelonnée pour optimiser l'impact de la campagne.

La formation Webroot® Security Awareness Training est une offre SaaS (Software-as-a-Service) entièrement basée sur le cloud. Les administrateurs peuvent gérer la formation et les simulations de phishing via la même console que Webroot® Business Endpoint Protection et Webroot® DNS Protection, offrant ainsi une expérience de « vitrine unique » avec une faible charge de gestion. Des utilisateurs bien formés réduiront le nombre d'incidents de sécurité auxquels une entreprise sera confrontée, ce qui, à son tour, réduira les coûts ainsi que les pertes en termes de productivité et de temps d'arrêt de l'entreprise. Selon nos observations de clients du monde réel, les entreprises qui utilisent la formation Webroot® Security Awareness Training parallèlement à la sécurité des terminaux rencontrent 20 % de logiciels malveillants en moins que celles qui ne déploient que notre protection des postes et n'ont aucune formation.

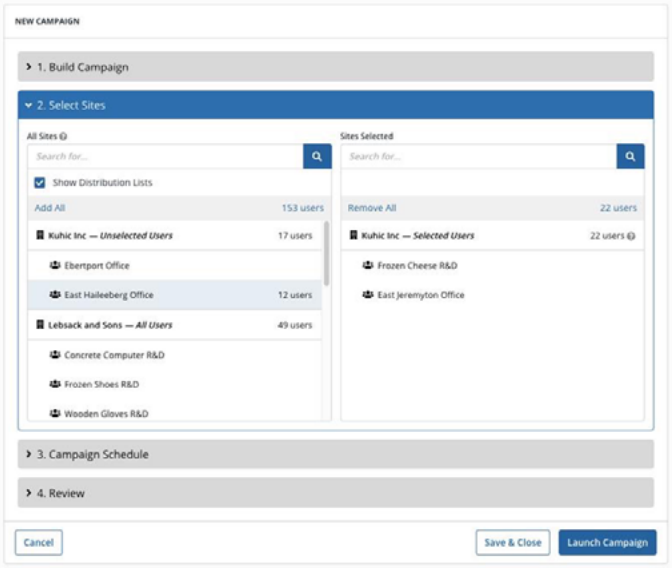
Avantages clés

- 20 % de logiciels malveillants en moins que les clients disposant uniquement de la protection des postes Webroot
- Des tâches administratives et une gestion des campagnes simplifiées
- Pertinence et fréquence élevées des mises à jour de la formation, avec un contenu utile, interactif et efficace
- Solution intégrée pour les MSP et les PME avec gestion multi-locataires
- Gestion automatisée de la formation et rapports de conformité au niveau de l'individu, du groupe et de l'entreprise.

Option de console unique et multi-clients qui vous permet d'organiser facilement des formations sur un seul site ou sur plusieurs sites

Principe de fonctionnement

La formation Webroot® Security Awareness Training comprend un système de gestion de l'apprentissage intuitif (LMS) hautement automatisé qui facilite la gestion de la formation. Grâce à l'intégration de Microsoft® Azure Active Directory, la formation Webroot® Security Awareness Training permet aux administrateurs d'automatiser l'importation des utilisateurs cibles et d'assurer leur synchronisation. L'assistant de configuration permet de créer facilement des simulations de phishing et des campagnes de formation. Quelques minutes suffisent pour nommer une campagne, sélectionner les destinataires souhaités, choisir le contenu et lancer la formation. Les administrateurs peuvent programmer une séquence de plusieurs formations et simulations de phishing sur une période donnée. En outre, les administrateurs qui gèrent plusieurs clients ou sites, comme les MSP, peuvent mettre en œuvre et gérer ces programmes pour différents clients à l'échelle mondiale. Les fonctions de programmation, de randomisation de l'heure de distribution, de rappels automatiques et de création de rapports permettent de gérer des campagnes de sensibilisation à la sécurité suivies et entièrement transparentes en toute facilité, qui améliorent efficacement le comportement des utilisateurs au fil du temps.



Console Formation de sensibilisation à la sécurité Webroot

L'intégration d'Azure AD simplifie la gestion de la formation des utilisateurs, tandis que l'assistant de campagne réduit le temps et les coûts consacrés à l'administration des programmes de formation à la cybersécurité. Le système LMS intégré assure le suivi de la participation de chaque utilisateur, de sorte que toute formation à la cybersécurité encourage la responsabilisation et que son impact est mesurable. Notre rapport de synthèse de la campagne met en évidence les données relative à la campagne et les résultats de la formation. Un tableau de bord de formation centralisé affiche toutes les campagnes en cours ou terminées, tandis qu'un flux de travail intuitif de gestion des campagnes permet aux administrateurs de concevoir et de lancer des formations multi-clients rapidement et facilement.

Webroot SAT comprend désormais Autopilot, un programme clé en main de sensibilisation à la sécurité dans lequel vous gérez la liste des utilisateurs ; nous envoyons chaque mois à ces derniers des formations et des campagnes de phishing.

Faire passer les utilisateurs finaux du statut de maillon faible de la chaîne de sécurité à celui de première ligne de cyberdéfense véritablement résiliente

Une formation continue, pertinente et mesurable pour minimiser les comportements à risque des utilisateurs et atteindre la cyber-résilience

OpenText Security Solutions rassemble les meilleures solutions pour aider votre entreprise à rester cyber-résiliente. Carbonite et Webroot peuvent vous aider à prévenir et à vous protéger contre les menaces qui se produisent en premier lieu, à minimiser l'impact en détectant et en répondant rapidement, à récupérer les données de manière transparente pour réduire l'impact, et à vous aider à vous adapter et à vous conformer aux réglementations changeantes.

Le vaste catalogue de formation Webroot® Security Awareness Training est mis à jour chaque mois pour couvrir une grande variété de thématiques liées à la sécurité et aux entreprises, dans différents formats. Vous pouvez recevoir des statistiques relatives aux campagnes de phishing et générer des rapports sur les activités pour chaque utilisateur ainsi que d'autres comptes-rendus afin d'évaluer la progression et le retour sur investissement. Dans une récente étude portant sur des simulations de phishing, 11 % des utilisateurs ont cliqué sur le premier e-mail de phishing. Avant la 6e simulation, le taux de clics était tombé à 6 % et avant la 18e simulation à 4 %. La formation Webroot® Security Awareness Training vous aide à renforcer la cyber-résilience des utilisateurs à un tarif forfaitaire avec les sujets recommandés par le NIST Cybersecurity Framework.

[1] Venure Beat 2021, Phishing attacks get smarter as targets struggle to keep up

opentext™ | Cybersecurity