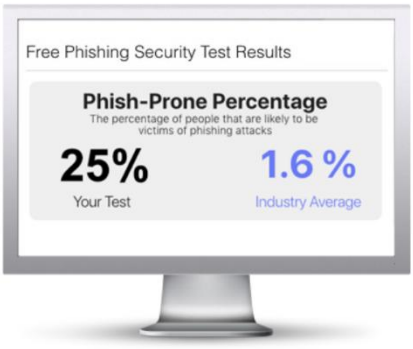
TESTEZ GRATUITEMENT VOTRE CYBERSÉCURITÉ GRÂCE AUX OUTILS DE CYBERSÉCURITÉ DE KnowBe4

Vous trouverez ci-dessous les liens pour obtenir les outils gratuits en fonction de la thématique.

Hameçonnage	Sensibilisation à la cybersécurité	Mots de passe	Sécurité des courriels	Détection de Malwares

Outils d'hameçonnage :

Saviez-vous que 91 % des violations de données réussies ont commencé par une attaque de spear phishing ?



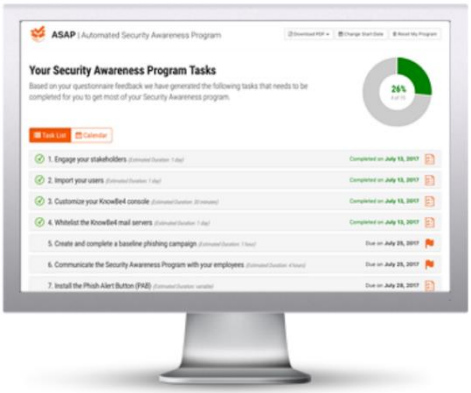
Découvrez quel pourcentage de vos employés sont Phish-prone™ avec votre test de sécurité phishing gratuit. De plus, comparez votre situation à celle de vos pairs grâce aux nouveaux critères d'évaluation de l'industrie du phishing !

Les professionnels de l'informatique ont compris qu'il était urgent de mettre en place des tests de phishing simulés pour renforcer la sécurité. Aujourd'hui, hameçonner ses propres utilisateurs est tout aussi important que d'avoir un antivirus et un pare-feu. C'est une pratique amusante et efficace de cybersécurité qui consiste à patcher votre dernière ligne de défense : LES UTILISATEURS

Inscrivez-vous, c'est gratuit !!

Test d'hameçonnage à blanc : https://bit.ly/3o5y4Qp
Test de réponse à un courriel d'hameçonnage : https://bit.ly/42XSgT9
Test d'hameçonnage sur les réseaux sociaux : https://bit.ly/3o3RaGy
Bouton d'alerte de suspicion : https://bit.ly/42X6Ji4
Deuxième chance : https://bit.ly/3MtARMI

Outils de sensibilisation à la cybersécurité :



De nombreux professionnels de l'informatique ne savent pas exactement par où commencer lorsqu'il s'agit de créer un programme de formation et de culture de la sensibilisation à la sécurité qui fonctionnera pour leur organisation.

Nous avons éliminé toutes les incertitudes grâce à notre outil gratuit de création de programme de sensibilisation à la sécurité automatisé (ASAP). ASAP est un outil révolutionnaire pour les professionnels de l'informatique qui vous aide à créer un programme de sensibilisation à la sécurité personnalisé pour votre organisation. ASAP vous montrera toutes les étapes nécessaires pour créer un programme de formation complet en seulement quelques minutes !

Le programme comprend des tâches réalisables, des conseils utiles, des suggestions de contenu de formation et un calendrier de gestion des tâches. Vous avez également la possibilité d'exporter le programme complet sous forme de version détaillée ou de résumé au format PDF**. Il s'agit d'un excellent outil pour vous aider à obtenir un budget pour votre programme et à faire un rapport à la direction.**

Inscrivez-vous, c'est gratuit !!

Aide à la planification du projet : https://bit.ly/3o5dfoi
Aperçu des modules de formations : https://bit.ly/3Igoh0D

Outils de sécurité pour le courrier électronique :

Combien d'informations d'identification de vos utilisateurs sont compromises ?

Un grand nombre d'adresses électroniques et d'identités de votre organisation sont exposées sur Internet et faciles à trouver pour les cybercriminels. Grâce à cette surface d'attaque, **ils peuvent lancer des attaques d'ingénierie sociale, de spear phishing et de ransomware contre votre organisation.**

La NOUVELLE version de l'Email Exposure Check Pro (EEC) de KnowBe4 identifie les utilisateurs à risque dans votre organisation en explorant les informations des médias sociaux d'entreprise et maintenant des milliers de bases de données de violations.

Nous vous enverrons par courrier électronique un rapport sommaire au format PDF indiquant le nombre d'e-mails exposés, les identités et les niveaux de risque trouvés. Vous recevrez également un lien vers le rapport détaillé complet des utilisateurs réels trouvés, y compris le nom de la violation et si un mot de passe a été exposé.

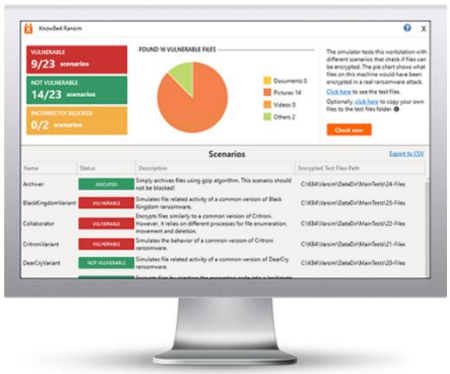
Inscrivez-vous, c'est gratuit !!

Vérification de l'exposition des adresses de courriel : https://bit.ly/41EuA5e
Test d'usurpation de domaine : https://bit.ly/3OaXDKB
Évaluation du serveur de messagerie : https://bit.ly/3O9G7Gx
Domaine « sosie » : https://bit.ly/3MtJ6rY

Outil de détection des malwares :

Votre protection des points finaux bloquera-t-elle réellement les infections par ransomware et cryptomining ?

Les acteurs malveillants proposent constamment de nouvelles versions de souches de ransomwares pour échapper à la détection. **Votre logiciel de protection des points d'accès est-il efficace pour bloquer les ransomwares lorsque les employés tombent dans le piège de l'ingénierie sociale ?**

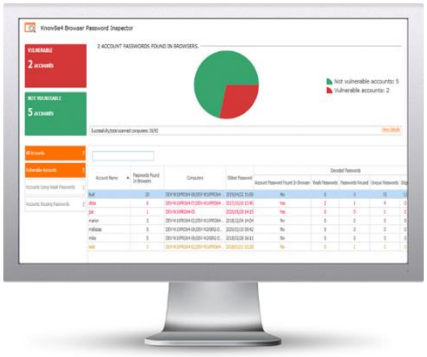


Le simulateur de ransomware "RanSim" de KnowBe4 vous permet d'évaluer rapidement l'efficacité de votre protection existante. RanSim simule 22 scénarios d'infection par ransomware et 1 scénario d'infection par cryptomining pour vous montrer si un poste de travail est vulnérable.

Inscrivez-vous, c'est gratuit !!

Simulateur de ransomware : https://bit.ly/3o2QSzP
Test de sécurité USB : https://bit.ly/3Mcq5cn

Mots de passe :



Lorsque vos utilisateurs enregistrent leurs mots de passe dans le navigateur, ils facilitent le piratage de votre réseau par les malfaiteurs.

Le récent rapport de Verizon sur les violations de données montre que les attaquants réussissent de mieux en mieux à voler les informations d'identification de vos utilisateurs en utilisant une combinaison de logiciels malveillants d'hameçonnage et d'extraction de mots de passe.

Une fois que les pirates ont obtenu l'accès, ils peuvent voler les noms d'utilisateur et les mots de passe de tous les comptes enregistrés dans les navigateurs. **Étant donné que 50 % des employés utilisent le même mot de passe** pour leurs comptes professionnels et personnels, le risque de vol d'informations d'identification et de prise de contrôle de comptes est encore plus grand !

Inscrivez-vous, c'est gratuit !!

Inspecteur de mot de passe du navigateur : https://bit.ly/3W60dn5
Test sur les mots de passe frauduleux : https://bit.ly/3ObwHtZ
Test de mot de passe faible : https://bit.ly/3BsE1tI
Test d'exposition au mot de passe : https://bit.ly/41AIaq8
Évaluation de la sécurité de l'authentification multifactorielle : https://bit.ly/3W5Qflz