Protection efficace des services en ligne et de la réputation

Kaspersky Takedown Service

kaspersky BRING ON THE FUTURE

Plus de 500

millions de tentatives d'accès à des sites Internet frauduleux ont été bloquées par les chercheurs de Kaspersky en 2022

20,000 $

le coût moyen des applications malveillantes pour Google Play sur le Dark Web

36,3 %

de toutes les attaques de phishing détectées par les technologies anti-phishing de Kaspersky en 2022 étaient liées au phishing financier

Défi

Les cybercriminels créent des domaines malveillants et de phishing, ainsi que des comptes de réseaux sociaux, utilisés pour attaquer votre entreprise et vos marques. L'incapacité d'atténuer ces menaces rapidement une fois identifiées peut conduire à une perte de revenus, à une atteinte à l'image de marque, à une perte de confiance des clients, à des fuites de données, et bien plus encore. Mais gérer les démontages de ce genre de domaines est un processus complexe qui requiert de l'expertise et du temps.

Qu'est-ce que Kaspersky Takedown ?

Kaspersky Takedown Service

Kaspersky bloque plus de 15 000 URL de phishing/d'escroqueries et empêche plus d'un million de tentatives de cliquer sur de telles URL chaque jour. Le service réduit rapidement les menaces posées par des comptes de réseaux sociaux malveillants avant qu'un quelconque dommage ne soit causé à la marque et à l'entreprise du client. Une gestion de bout en bout des tâches permettant une action rapide pour minimiser votre risque numérique afin que votre équipe puisse se concentrer sur d'autres tâches prioritaires.

Kaspersky fournit à ses clients une protection efficace de leurs services en ligne et de leur réputation en collaborant avec des organisations internationales ainsi que des organismes nationaux et régionaux chargés de l'application de la loi :

- INTERPOL
- Europol
- L'unité Microsoft Digital Crimes
- L'unité nationale de lutte contre la criminalité liée à la haute technologie (NHTCU) des services de police néerlandais
- La Police de la Cité de Londres
- Des équipes Computer Emergency Response Teams (CERT) dans le monde entier

Comment ça fonctionne ?

1

Envoyez vos demandes via Kaspersky Company Account, notre portail de support pour les entreprises clientes

2

Nous préparerons toute la documentation nécessaire et enverrons la demande de démontage à l'autorité locale / régionale compétente (CERT, registraire, etc.) ayant les droits juridiques nécessaires pour fermer le domaine

3

Vous recevrez des notifications à chaque étape du processus jusqu'à ce que la ressource demandée soit démontée avec succès

Pourquoi choisir Kaspersky Takedown ?

Protection mondiale

Peu importe où est enregistré le domaine malveillant ou de phishing, Kaspersky demandera son démontage de l'organisation locale avec l'autorité juridique pertinente

Gestion intégrale

Nous nous occuperons de tout le processus de démontage et réduirons au maximum votre implication

Kaspersky Digital Footprint Intelligence

Le service est conçu pour fournir aux clients une analyse de leur empreinte dans les réseaux ouverts et une vue d'ensemble des possibilités offertes aux adversaires

Intégration avec Digital Footprint Intelligence

Kaspersky Takedown Service peut être acheté séparément, mais son intégration à Kaspersky Digital Footprint Intelligence permet de tirer le meilleur parti de la synergie naturelle entre ces services. Kaspersky Digital Footprint Intelligence fournit des notifications en temps réel à propos des domaines de phishing et de programmes malveillants qui peuvent être immédiatement envoyés à Kaspersky Takedown Service en vue d'un blocage ultérieur

Visibilité complète

Vous serez informés à chaque étape du processus, de l'enregistrement de votre demande au démontage accompli

Kaspersky Takedown Service

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture