Protección eficaz de los servicios en línea y de la reputación

Kaspersky Takedown Service

kaspersky BRING ON THE FUTURE

Más de 500

millones de intentos de acceder a sitios web fraudulentos fueron bloqueados por los investigadores de Kaspersky en 2022.

$20 000

de costo promedio de las aplicaciones maliciosas para Google Play en la red oscura.

36.3 %

de todos los ataques de phishing detectados por las tecnologías antiphishing de Kaspersky en 2022 estaban relacionados con el phishing financiero.

Desafío

Los ciberdelincuentes crean dominios maliciosos y de phishing, así como cuentas en redes sociales, que se usan para atacar a su empresa y sus marcas. La incapacidad para mitigar estas amenazas con rapidez, una vez identificadas, puede provocar una pérdida de ingresos, daños a la marca, pérdida de confianza de los clientes, filtraciones de datos, y mucho más. De todos modos, gestionar el ataque de estos dominios es un proceso complejo que requiere experiencia y tiempo.

Qué es Kaspersky Takedown

Kaspersky Takedown Service

Kaspersky bloquea más de 15 000 direcciones URL de phishing o estafas, y evita más de un millón de intentos de hacer clic en este tipo de URL cada día. El servicio también mitiga con rapidez las amenazas que plantean las cuentas maliciosas en redes sociales antes de que pueda causarle daño a la marca y la empresa de un cliente. Nos ocuparemos de gestionar su eliminación y permitiremos acciones rápidas para minimizar los riesgos digitales, a fin de que su equipo pueda concentrarse en otras tareas prioritarias.

Kaspersky ofrece a sus clientes una protección eficaz de sus servicios en línea y de su reputación colaborando con organizaciones internacionales y agencias de seguridad nacionales y regionales:

- Interpol
- Europol
- Unidad de delitos digitales de Microsoft
- Unidad nacional de delitos de alta tecnología (NHTCU) de la Policía Nacional de los Países Bajos
- Policía de la ciudad de Londres
- Equipo de respuesta ante emergencias informáticas (CERT) en todo el mundo

Cómo funciona

1

Envíe sus solicitudes a través de Kaspersky CompanyAccount, nuestro portal corporativo de atención al cliente.

2

Prepararemos toda la documentación necesaria y enviaremos la solicitud de eliminación a la autoridad local o regional pertinente (CERT, registro, etc.) que tenga los derechos legales necesarios para cerrar el dominio.

3

Recibirá notificaciones en cada paso del proceso hasta que el recurso solicitado se elimine con éxito.

Por qué elegir Kaspersky Takedown

Cobertura mundial

No importa dónde esté registrado un dominio malicioso o de phishing, Kaspersky solicitará su eliminación a la organización regional con la autoridad legal pertinente.

Administración integral

Gestionaremos todo el proceso de eliminación y minimizaremos su participación.

Kaspersky Digital Footprint Intelligence

El servicio está diseñado para proporcionar a los clientes un análisis de su huella en las redes abiertas y una visión general de las oportunidades que se presentan a los adversarios.

Integración con Digital Footprint Intelligence

Kaspersky Takedown Service puede comprarse por separado, pero su integración con Kaspersky Digital Footprint Intelligence aprovecha al máximo la sinergia natural entre estos servicios. Kaspersky Digital Footprint Intelligence envía notificaciones en tiempo real sobre dominios de phishing y malware que pueden enviarse de inmediato a Kaspersky Takedown Service para su bloqueo.

Visibilidad completa

Se le informará en cada fase del proceso, desde el registro de su solicitud hasta la eliminación exitosa.

Kaspersky Takedown Service

Más información

latam.kaspersky.com

#kaspersky
#bringonthefuture