



Proteção eficaz para seus  
serviços online e a reputação  
da sua empresa

# Kaspersky Takedown Service

> 500

milhões de tentativas de acesso a sites fraudulentos foram bloqueadas pelos pesquisadores da Kaspersky em 2022

USD 20.000

é o custo médio de aplicativos maliciosos para o Google Play na dark web

36,3%

de todos os ataques de phishing detectados pelas tecnologias antiphishing Kaspersky em 2022 estiveram relacionados a phishing financeiro

---

## Desafio

Os cibercriminosos criam domínios maliciosos e de phishing, bem como contas falsas em redes sociais, que são usados para atacar sua empresa e sua marca. A incapacidade de eliminar rapidamente essas ameaças, após serem identificadas, pode levar à perda de receita, danos à marca, perda de confiança dos clientes, vazamentos de dados e muito mais. Porém, gerenciar a remoção desses domínios é um processo complexo, que requer experiência e tempo.

---

## O que é o Kaspersky Takedown?



### Kaspersky Takedown Service

A Kaspersky bloqueia mais de 15 mil URLs de phishing/scam e impede mais de um milhão de tentativas de acesso a esses URLs todos os dias. O serviço elimina rapidamente as ameaças representadas por contas de redes sociais maliciosas antes que qualquer dano possa ser causado à marca e aos negócios de um cliente. Cuidaremos do seu gerenciamento de remoção e permitiremos uma ação rápida para minimizar seu risco digital para que sua equipe possa se concentrar em outras tarefas prioritárias.

A Kaspersky oferece aos seus clientes uma proteção eficaz de seus serviços online e reputação, trabalhando com organizações internacionais, agências nacionais e regionais de execução da lei:

- INTERPOL
- Europol
- Unidade de Crimes Digitais da Microsoft
- A Unidade Nacional de Combate aos Crimes de Alta Tecnologia (NHTCU) da Agência Policial da Holanda
- A Polícia da Cidade de Londres
- Equipes Mundiais de Respostas às Emergências em Computadores (CERTs)

---

## Como funciona?

1

Você pode solicitar diretamente através de uma Conta Corporativa Kaspersky, no nosso portal de suporte ao cliente corporativo.

2

Prepararemos toda a documentação necessária e enviaremos a solicitação de remoção à autoridade local/regional relevante (CERT, registrador, etc.) que tenha os direitos legais necessários para encerrar o domínio.

3

Você receberá notificações em todas as etapas até que o recurso solicitado seja removido com sucesso.

---

## Por que escolher a Kaspersky?



### Cobertura global

Seja qual for o local em que um domínio malicioso ou de phishing esteja registrado, a Kaspersky solicitará sua remoção da organização regional com a autoridade legal relevante.



### Gerenciamento de ponta a ponta

Gerenciaremos todo o processo de remoção e minimizaremos seu envolvimento.



### Kaspersky Digital Footprint Intelligence

O serviço é projetado para fornecer aos clientes uma análise de presença em redes abertas e uma visão geral das oportunidades de ataque dos adversários



### Integração com Digital Footprint Intelligence

O Kaspersky Takedown Service pode ser adquirido separadamente, mas sua integração com o Kaspersky Digital Footprint Intelligence garante ao máximo a efetividade natural entre esses serviços. O Kaspersky Digital Footprint Intelligence fornece notificações em tempo real sobre domínios de phishing e malware, que podem ser imediatamente enviados ao Kaspersky Takedown Service para bloqueamento instantâneo.



### Visibilidade completa

Você será notificado em cada etapa do processo, desde o registro da sua solicitação até a remoção bem-sucedida.



# Kaspersky Takedown Service

Saiba mais

[www.kaspersky.com.br](http://www.kaspersky.com.br)

© 2023 AO Kaspersky Lab.  
As marcas comerciais registradas e as marcas de serviço  
pertencem aos seus respectivos proprietários.

#kaspersky  
#bringonthefuture