



Effective protection of online
services and reputation

Kaspersky Takedown Service

> 500

million attempts at accessing fraudulent websites were blocked by Kaspersky researchers in 2022

\$20,000

the average cost of malicious apps for Google Play on the dark web

36,3%

of all phishing attacks detected by Kaspersky anti-phishing technologies in 2022 were related to financial phishing

Challenge

Cybercriminals create malicious and phishing domains, as well as social media accounts, which are used to attack your company and your brands. The inability to quickly mitigate these threats, once identified, can lead to a loss of revenue, brand damage, loss of customer trust, data leaks, and more. But managing takedowns of these domains is a complex process that requires expertise and time.

What is Kaspersky Takedown



Kaspersky Takedown Service

Kaspersky blocks more than 15 000 phishing / scam URLs and prevents over a million attempts clicking such URLs every single day. The service also quickly mitigates threats posed by malicious social media accounts and fake mobile apps published on marketplaces before any damage can be caused to a customer's brand and business. We'll take care of your takedown management and enable swift action to minimize your digital risk so your team can focus on other priority tasks.

Kaspersky provides its customers with effective protection of their online services and reputation by working with international organizations, national and regional law enforcement agencies:

- INTERPOL
- Europol
- Microsoft Digital Crimes Unit
- The National High-Tech Crime Unit (NHTCU) of the Netherlands' Police Agency
- The City of London Police
- Computer Emergency Response Teams (CERTs) worldwide

How it works

1

Submit your requests via Kaspersky Company Account, our corporate customer support portal

2

We will prepare all the necessary documentation and will send the request for takedown to the relevant local / regional authority (CERT, registrar, etc.) that has the necessary legal rights to shut down the domain

3

You will receive notifications at every step of the way until the requested resource is successfully taken down

Why choose Kaspersky Takedown



Global coverage

It doesn't matter where a malicious or phishing domain is registered, Kaspersky will request its takedown from the regional organization with the relevant legal authority



End-to-end management

We will manage the entire takedown process and minimize your involvement



Kaspersky Digital Footprint Intelligence

The service is designed to provide customers with an analysis of their footprint in open networks and an overview of the opportunities presented to adversaries



Integration with Digital Footprint Intelligence

Kaspersky Takedown Service can be purchased separately, but its integration with Kaspersky Digital Footprint Intelligence makes the most of the natural synergy between these services. Kaspersky Digital Footprint Intelligence provides real-time notifications about phishing and malware domains which can be immediately submitted to Kaspersky Takedown Service for further blocking



Complete visibility

You will be notified at each stage of the process, from registration of your request to a successful takedown



Kaspersky Takedown Service

[Learn more](#)

www.kaspersky.com

© 2023 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#bringonthefuture