Kaspersky Takedown Service

kaspersky BRING ON THE FUTURE

Kaspersky Takedown Service

Service benefits

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.

Complete visibility

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

Integration with Digital Footprint Intelligence

The service integrates with Kaspersky Digital Footprint Intelligence which provides real-time notifications about phishing and malware domains, designed to damage, abuse or impersonate your brand / organization. A single solution is an important component of a comprehensive cybersecurity strategy.

Challenge

Cybercriminals create malicious and phishing domains 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.

Solution

Kaspersky blocks more than 15 000 phishing/scam URLs and prevents over a million attempts clicking such URLs every single day. Our many years of experience in analyzing malicious and phishing domains means we know how to collect all the necessary evidence to prove that they are malicious. 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 (e.g. INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High-Tech Crime Unit (NHTCU) of the Netherlands' Police Agency and The City of London Police), as well as Computer Emergency Response Teams (CERTs) worldwide.

How it works

You can submit your requests via Kaspersky Company Account, our corporate customer support portal. 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. You will receive notifications at every step of the way until the requested resource is successfully taken down.

Effortless protection

The Kaspersky Takedown Service quickly mitigates threats posed by malicious and phishing domains before any damage can be caused to your brand and business. End-to-end management of the entire process saves you valuable time and resources.

Learn more

Kaspersky
Threat Intelligence

www.kaspersky.com