Success Stories

1k-a-Day: Real Takedown Cases Showing How Leading Brands Stop Threats with Axur

When dealing with digital threats, speed and accuracy matter. Every extra minute a phishing site or fraudulent ad remains active poses serious risks to your brand and customers.

Axur's takedown solution proactively identifies and neutralizes threats, empowering your team to stay ahead without the need for additional cybersecurity resources.

Real Stories of Axur's Takedown Success

Yes, these timelines are real — so are the response times.

Multi-Point Phishing Threat

- Axur detected a phishing URL connected to a fraudulent Meta ad impersonating a client's brand.
  10:56 AM
- Web Safe Reporting technology instantly notified 15 entities, including ISPs and domain registrars, triggering red alert screens to warn users about the phishing threat.
  10:56 AM
- Phishing URL neutralized within just 20 minutes.
  11:16 AM
- Fraudulent ad neutralized in under 10 hours.
  09:16 PM
- **Solved!** Takedown finished.
  09:16 PM

Phishing ad targeting **airline** customers blocked.

High-Risk Social Media Profile

- Our system flagged a high-risk fake social profile on Facebook using advanced machine learning.
  08:45 AM
- Customer approved the takedown request.
  09:35 AM
- Automated notification sent to Meta.
  09:51 AM
- Meta confirmed the removal of the fake profile.
  10:15 AM
- **Solved!** Takedown finished.
  10:15 AM

E-commerce giant stops fake Facebook profile with seamless automation.

Initially Inactive Phishing Threat

- A phishing URL was detected but initially marked inactive.
  02:12 AM
- The URL became active; Axur's platform automatically flagged it for the customer.
  04:28 AM
- One-click takedown initiated; ISP automatically alerted.
  04:28 AM
- **Solved!** Takedown finished.
  04:54 AM

E-commerce brand targeted by phishing campaign hosted on a previously parked domain.

Takedown with automated follow-up==-=mn

- One-click Takedown requested.
  06:00 PM
- After a follow-up notification, Meta acknowledged additional information was needed.
  05:51 PM
- Axur automatically supplied necessary data, leading to same-day removal.
  07:51 PM
- **Solved!** Takedown finished.
  07:51 PM

Financial services firm quickly removed a fake Facebook profile posing as official support.

Fraudulent Ad Detected and Neutralized

- A fraudulent ad was identified via our Meta Ads collector.
  08:33 AM
- Takedown requested automatically by our system.
  09:10 AM
- Meta confirmed the ad was removed.
  10:05 AM
- **Solved!** Takedown finished.
  10:05 AM

E-commerce brand quickly neutralizes fraudulent ads—minimizing risk to customers.

Illegal Product Listing on Marketplace

- Automated detection of a prohibited product listing.
  05:19 PM
- Alert sent through Axur's exclusive API and marketplace trust.
  05:27 PM
- Listing removed, marketplace alerted other sellers.
  05:41 PM
- **Solved!** Takedown finished.
  05:41 PM

Government agency eliminates illegal product listing in only 14 minutes.

Phishing URL Using Customer Branding

- Our platform detected a phishing URL impersonating the client's website.
  02:12 AM
- Takedown requested automatically
  10:54 AM
- Web Safe Reporting technology instantly alerted 15 entities, activating red warning screens on phishing threats.
  10:54 AM
- Registrar confirmed the URL was removed.
  11:14 AM
- **Solved!** Takedown finished.
  11:14 AM

Beauty e-commerce site neutralizes phishing threat in just 49 minutes.

Fully Automated Social Media Ad Takedown

- Incident automatically created and triaged.
  07:28 PM
- Automatic takedown request sent to Meta.
  07:36 PM
- The ad was inaccessible.
  08:27 PM
- **Solved!** Takedown finished.
  08:27 PM

Financial institution removes fake Facebook ad in just 51 minutes.

///AXUR

Spot them. *Stop* them. Take them down.

Why Speed and Automation Matter

Imagine waking up to discover a fake ad or phishing page impersonating your brand. With Axur, you don't have to wait until business hours or rely on manual intervention. Our automated systems proactively detect, flag, and notify relevant entities within minutes, often resolving threats before they escalate.

→ **Reduce exposure time—minimize brand damage and prevent customer loss. With a median uptime of just 9 hours, you're never left waiting days for resolution.**

Tailored Responses for Diverse Threats

Not all threats look alike. Whether you're dealing with a phishing URL, fraudulent ad, or prohibited product listing, Axur's platform adapts intelligently to the specific scenario.

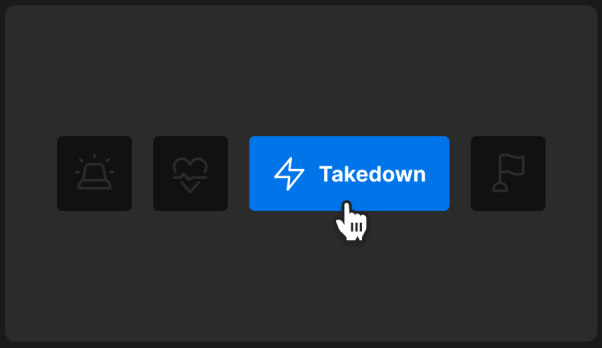
We alert ISPs, marketplaces, and social media platforms using customized protocols, ensuring faster, more effective takedowns.

→ **Comprehensive protection—covering multiple attack vectors, so you're confidently protected across all digital channels.**

Transparency and Control in Every Step

You shouldn't have to guess about the status of your takedowns. Axur delivers full transparency, from initial detection to complete resolution, with clear timelines and regular progress updates.

→ **Gain confidence in your security processes and maintain thorough documentation to support compliance or legal actions when necessary.**



The Axur Difference

Automated Intelligence

Our advanced machine-learning models analyze and identify threats with unmatched accuracy, flagging risks before they can spread.

Global Reach, Local Expertise

With direct connections to over 400 ISPs across five continents, we ensure swift and effective action—no matter where the threat arises.

Web Safe Reporting

Beyond takedowns, our Web Safe Reporting instantly alerts relevant entities, enabling protective measures like browser warnings on active phishing sites.

Protect your brand, your customers, and your reputation—faster than ever.

Gartner Peer Insights 5/5

DISCOVER THE BEST TAKEDOWN

///AXUR