topDNS Best Practice Series Part 8:
Handling Abuse Reports and Takedowns

On 25 February 2025, **Spamhaus, Team Internet & eco's topDNS Initiative** hosted the eighth in a series of topDNS Best Practice webinars highlighting what the domain name industry is doing to fight DNS abuse.

In the Best Practices for Handling Abuse Reports and Takedowns webinar, **Volker Greimann**, Head of Policy and Compliance, General Counsel - Online Division at **Team Internet**, and **Sven Krohlas**, Data Analyst at Spamhaus, discussed the challenges faced in abuse reporting, common pitfalls, and strategies to ensure efficient reporting.

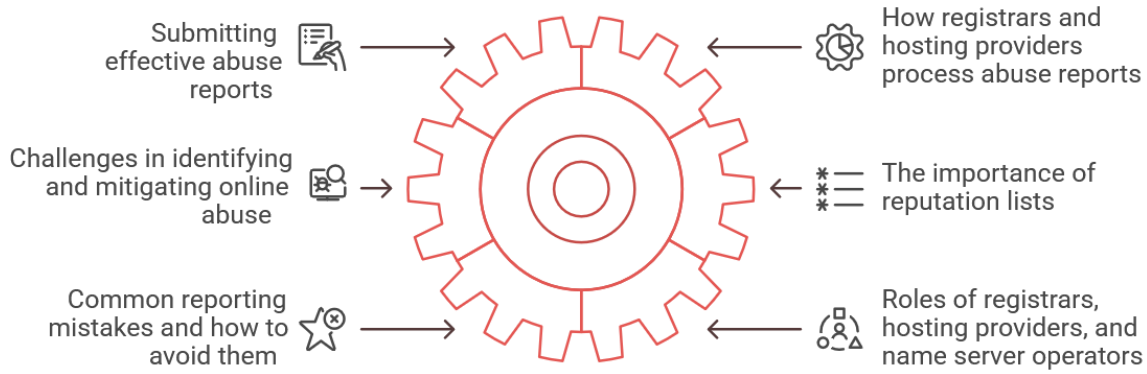

Figure 1: The Best Practices for Handling Abuse Reports and Takedowns webinar

They explored the evolving landscape of abuse reporting, stressing the need for structured, clear reports to enable faster resolutions. Effective communication and collaboration between abuse reporters and service providers were also identified as essential for timely takedowns.

Best practices for reporting abuse

Sven Krohlas emphasised the importance of clarity in abuse reports, stating that one of the biggest barriers to effective takedowns is poorly structured submissions. He explained that abuse reports often lack essential details, causing delays and inefficiencies in the response process. Including specific evidence such as screenshots, HTTP logs, and geo-location data can significantly improve the effectiveness of an abuse report. Additionally, he highlighted that clear communication within reports reduces unnecessary back-and-forth queries between reporters and abuse-handling teams, saving valuable time.

"Reputation list providers are always interested in your reports.
They play a crucial role in expediting takedowns and minimizing harm."

Another key point raised by Krohlas was the necessity of providing machine-readable data to ensure automation-friendly processing. He noted that abuse departments rely on automated

tools to sort and prioritise reports, and reports in formats like X-ARF allow for faster response times. Structured data ensures that abuse-handling systems can parse and classify reports efficiently, leading to quicker resolution times. Furthermore, he mentioned that some registrars and hosting providers are moving towards automated decision-making processes, where structured reports with relevant metadata play a crucial role in determining takedown actions.

Figure 2: Best practices for reporting abuse

Krohlas also underlined the role of proactive engagement with hosting providers and registrars. He explained that those reporting abuse should not only focus on sending complaints but also on establishing trust with service providers. Reporters who consistently submit well-structured, verifiable reports are more likely to receive prompt action compared to those who provide vague or incomplete information.

"The goal should be to make reports as easy to process as possible. A well-structured, clear report can be the difference between a fast takedown and an unresolved issue."

He reiterated that fostering a cooperative relationship with anti-abuse teams leads to a more streamlined and efficient abuse-handling process.

Registrar perspective on abuse handling

Volker Greimann discussed the internal process of registrars when handling abuse complaints.

"We prioritise efficiency:
last in, first out processing allows us to take down active threats quickly."

He elaborated on the practicalities of abuse handling from a registrar's perspective, explaining that prioritisation is essential when processing reports. He emphasised that registrars must balance multiple obligations, from responding to abuse complaints quickly to ensuring that legitimate customers are not unfairly impacted. Registrars follow structured workflows, often

prioritising malware and phishing cases above other types of abuse, as these pose the most immediate risks to users.

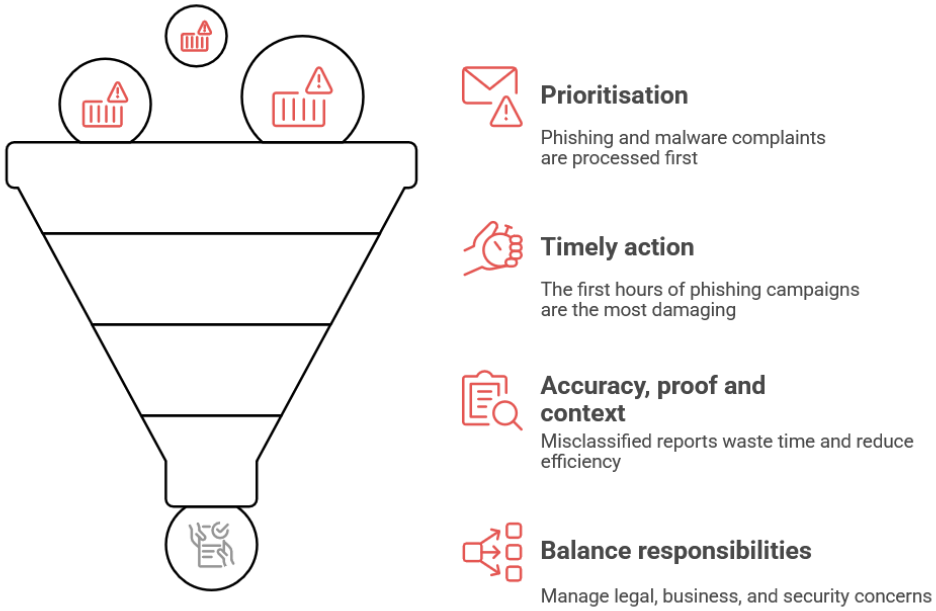

Figure 3: The registrar perspective on abuse handling

Greimann also pointed out that automation and enrichment tools are becoming indispensable in abuse management. Registrars increasingly rely on external reputation services to verify abuse claims efficiently. These services help identify patterns of malicious activity, allowing registrars to take swift action against domains used for phishing or malware distribution. He noted that registrars must stay ahead of abuse tactics by continuously updating their detection and mitigation strategies.

"A well-documented, evidence-based abuse report significantly reduces processing time. The clearer the report, the faster we can act."

Additionally, he stressed the importance of responsible enforcement actions. Registrars must carefully evaluate each abuse case to ensure that legitimate businesses are not mistakenly disrupted. Misclassification or overzealous takedowns can damage trust in the industry and lead to legal disputes. Greimann advocated for open communication between registrars, abuse reporters, and service providers to create a transparent and effective abuse-handling ecosystem.

Key takeaways

- Effective reporting leads to faster takedowns.
- Reputation lists are essential tools in cybersecurity.
- Coordinated communication with registrars and hosts improves response times.
- Web forms hinder scalability; APIs and automated tools should be prioritised.
- Registrars have limitations; targeted reporting is necessary.

The webinar highlighted the increasing complexity of abuse management and the need for structured, evidence-backed reports. Collaboration among industry stakeholders, including registrars, hosting providers, and cybersecurity experts, remains crucial in mitigating online abuse.

Automation is key to improving efficiency. Machine-readable reports and external reputation services help registrars handle abuse cases faster while minimising errors. Implementing such technologies ensures quicker response times and better accuracy in identifying threats.

Stronger industry cooperation and awareness of best practices will be vital moving forward. Continued engagement through webinars, policy discussions, and collaborative efforts will help create a more secure and resilient Internet ecosystem.

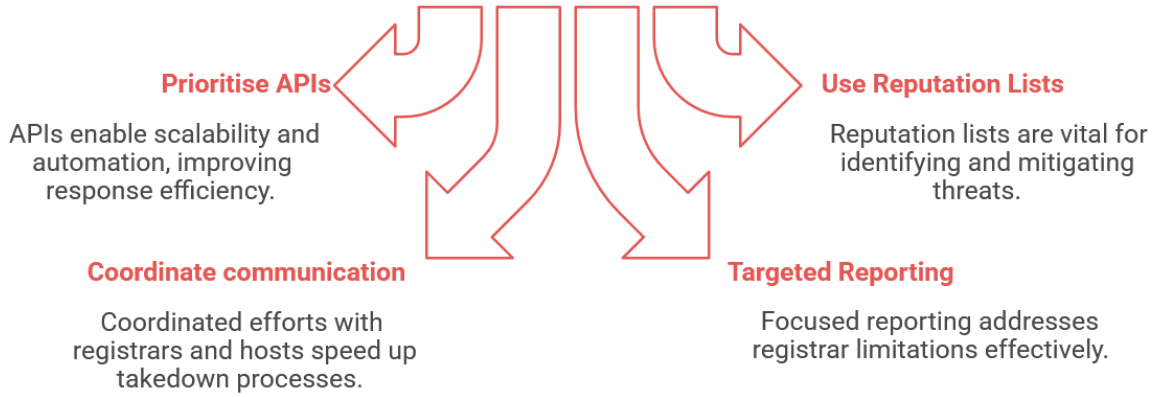

Figure 4: Best practices for handling abuse reports and takedowns

Webinar recording:
Best Practices for Handling Abuse Reports and Takedowns (for eco members only)

Previous webinars in the topDNS Best Practice series are available on the topDNS website: https://topdns.eco.de/.

FOR SOCIAL MEDIA etc.

Sven Krohlas, Data Analyst at Spamhaus, on how to make abuse reports more effective:

- **Provide Proof:** Include screenshots, HTTP logs, and relevant technical data.
- **Give Context:** Mention geo-location, user agents, and any cloaking mechanisms.

- **Use Machine-Readable Formats:** Avoid obfuscation and use standard formats like X-ARF.
- **Avoid Legal Jargon:** Reports should be technical and to the point to avoid delays.
- **Identify the Correct Party:** Reporting should be directed to the appropriate stakeholders (registrars, hosts, name server operators, etc.).
- **Engage with Anti-Abuse Teams as Partners:** Maintain professionalism and avoid adversarial tones.

Read more on https://topdns.eco.de/

Registrar Perspective on Abuse Handling

Volker Greimann, Head of Policy and Compliance, General Counsel - Online Division at Team Internet, on the internal process of registrars when handling abuse complaints:

- **Prioritisation Matters:** Phishing and malware complaints are processed first.
- **Timely Action is Critical:** The first hours of phishing campaigns are the most damaging.
- **Avoiding Misreporting:** Misclassified reports waste time and reduce efficiency.
- **Registrar's Responsibilities:** They must balance legal obligations, business considerations, and security concerns.

Read more on https://topdns.eco.de/

Key Takeaways

Sven Krohlas, Data Analyst at Spamhaus, and **Volker Greimann**, Head of Policy and Compliance, General Counsel - Online Division at **Team Internet**, on Best Practices for Handling Abuse Reports and Takedowns:

- Effective reporting leads to faster takedowns.
- Reputation lists are essential tools in cybersecurity.
- Coordinated communication with registrars and hosts improves response times.
- Web forms hinder scalability; APIs and automated tools should be prioritised.
- Registrars have limitations; targeted reporting is necessary.