

# STATE OF THE DNS



Why Preventing, Mitigating  
& Fighting Abuse Concerns  
Everyone



Fighting the Good Fight:  
Preventing the Spread  
of CSAM With Software



Mitigating DNS abuse:  
Taking a Firm Position and  
Protecting Employees



Borderless Fight  
Against Illegal Content



Abuse Management for  
Domain Names

powered by



We thank the members of the  
topDNS Steering Committee for their support



Learn more about topDNS: [topdns.eco](https://topdns.eco)

## CONTRIBUTORS TO THIS ISSUE



Thomas Rickert  
 Director, eco Names  
 & Numbers Forum,  
 Attorney-at-Law, Rickert  
 Rechtsanwaltsgesellschaft



Lars Steffen  
 Director, eco International,  
 eco – Association of the  
 Internet Industry



Simone Catania  
 Global Content &  
 Communications  
 Manager, InterNetX



Lars "LG" Forsberg  
 Chief Technology Officer,  
 iQ



Michele Neylon  
 CEO, Blacknight



Theo Geurts  
 GRC/Privacy Officer,  
 Realtime Register



Inma del Rosal Mendez  
 Senior Director Channel  
 Services, PIR (Public  
 Interest Registry)



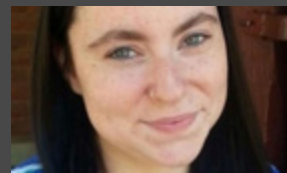
Brian Cimboric  
 Vice President, General  
 Counsel, PIR (Public  
 Interest Registry)



Alastair Gill  
 Journalist and Editor



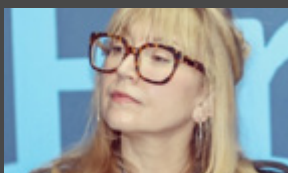
Patrick Ben Koetter  
 Leader of the Email and  
 Anti-Abuse Competence  
 Groups, eco Association,  
 Member of the Board,  
 sys4 AG



Natasha Pelham-Lacey  
 Security Analyst,  
 CleanDNS



Gia Isabella  
 Abuse Program Manager,  
 CleanDNS



Kelly Hardy  
 Head of Registry Policy,  
 CentralNic



Verena Kuthe  
 Head of Sales & Business  
 Development, LEMARIT



Katrin Ohlmer  
 Managing Director,  
 DOTZON



Alexandra Koch-Skiba  
 Head of the eco  
 Complaints Office,  
 eco - Association of the  
 Internet Industry



Els de Jong  
 Marketing Coordinator,  
 BIT



Wido Potters  
 Board Member, AbuseIO  
 Foundation; Manager  
 support & sales, BIT

Please note: The opinions expressed in Industry Insights published by dotmagazine are the author's own and do not reflect the view of the publisher, eco – Association of the Internet Industry

# CONTENTS



Contributors to this Issue	3
Contents	4
Editorial	6
Editorial Team	6
Why Preventing, Mitigating & Fighting Abuse Concerns Everyone	8
The Debate Around Defining, Preventing and Mitigating DNS abuse	10
DNS abuse: Everyone's Problem	13
Cleaning up the Neighborhood	16
Gaining More Insight into Malicious Domains	19
QPI: A "Call To Arms" on Responsible Growth	22
Not in Our Domain: How EURid is Using AI and Global Cooperation to Tackle Cybercrime	25
Email Blocklists for Real-Time Detection and Mitigation	28







Let's End Counter-Productive Anti DNS abuse Reporting	32
Evidence Equals Better DNS abuse Mitigation	34
Mitigating DNS abuse: Taking a Firm Position and Protecting Employees	36
Control Your Digital Brand: On the Interplay of Defensive Domain Registrations, Active Monitoring, and Brand Enforcement	38
Abuse Management for Domain Names	41
Vigilance of Society Against Illegal Content	43
Fighting the Good Fight: Preventing the Spread of CSAM With Software	45
Congratulations on Your New Business – We Need to Talk	47
Borderless Fight Against Illegal Content	51
Adding Trust & Security to Internet Interactions with DNSSEC	55
About eco	58
Publication Details	58



## EDITORIAL



Thomas Rickert, Director, eco Names & Numbers Forum, Attorney-at-Law, Rickert Rechtsanwalts-gesellschaft

Dear reader,

**Technical developments are, by their nature and by their dynamics, always faster than the developments legislators could ever achieve. Moreover, the Internet is borderless. It is a global tool that can be used by almost anyone around the globe, whereas legislative initiatives usually have only national reach. And that is why it's always good for an industry to come up with ideas on how to respond with appropriate measures to the challenges it is facing.**

The DNS has proven to be the foundation for the global expansion of the Internet as a universal public resource. However, like every innovation and every technology, the Internet and the DNS are facing abuse. This special edition of dotmagazine looks at various types of abuse and industry initiatives to combat them. The task of tackling and preventing abuse on the Internet is a complex one, one which needs to avoid overblocking and collateral damage to freedom and diversity of speech.

The excellent authors of this issue provide a broad overview of the different forms and definitions of abuse and best practice approaches for how to mitigate and fight some of them.



Lars Steffen, Director, eco International, eco – Association of the Internet Industry

eco's most recent contribution to this issue is the topDNS Initiative to work on what some define as DNS abuse – which is, in fact, closely connected to multiple other types of abuse. Our goal is to bring all relevant stakeholders and intermediaries to the table and put up for discussion all different types of abuse that harm everyone on the Internet, to initiate a discussion about roles and responsibilities across the board with the entire industry.

But what is DNS abuse? Simone Catania from InterNetX takes on the task of defining and delineating DNS abuse in terms of harmful or illegal activities that exploit the DNS. With awareness comes the ability to act, says Lars Forsberg from iQ and looks at the need for awareness of DNS abuse, especially of the new gTLDs. Michele Neylon, CEO of Blacknight, echoes the need for awareness and explains why cleaning up the neighborhood is a worthwhile activity to make the Internet a place people want to do business in.

When it comes to malicious domains, Theo Geurts from RealtimeRegister B.V. explores the advantages of taking a proactive approach to their mitigation, introducing a tool that enables predictions to be made on the basis of gathered, analyzed, and visualized data to prevent malicious registrations before they occur. Positive reinforcement and (financial) incentives for good behavior are key to the approach of Inma

## EDITORIAL TEAM



Lars Steffen  
eco – Association of the Internet Industry



Judith Ellis  
eco – Association of the Internet Industry



Eilín Geraghty  
eco – Association of the Internet Industry



Cáit Kinsella  
eco – Association of the Internet Industry



Ladan Raeisian  
eco – Association of the Internet Industry



Source: © royyimzy | iStockphoto

Del Rosal Mendez and Brian Cimboric from PIR (Public Interest Registry), who examine the positive impact on growth and reduction in abuse rates for .ORG registrations through the use of their Quality Performance Index (QPI). Equally, EURid's answer to keeping on top of abusive domain registrations is the eco award-winning Abuse Prevention and Early Warning System (APEWS), which uses AI and professionally curated incident lists to analyze potentially abusive domain names and delay their registration – catching them before they can be used to carry out any attacks. Patrick Ben Koetter from the eco Email and Anti-Abuse Competence Groups also explains the value of reputation and how blocklists and allowlists help with real-time detection and mitigation.

Even just reporting abuse is difficult enough, as Natasha Pelham-Lacey from CleanDNS points out: She recommends digital infrastructure and DNS providers adopt consistent and realistic standards for proof to lower the bar for the complainant and increase the speed and efficiency of takedowns. Her CleanDNS colleague Gia Isabella looks at the importance of supplying evidence as part of the process of combatting DNS abuse – and the need for standardization of the kind of evidence required.

Unfortunately, abusive activities on the Internet often involve fraud and copyright infringements. Kelly Hardy from CentralNic provides cybercrime advice for end customers and clients operating businesses online. Verena Kuthe from LEMARIT puts the onus on brand owners to adopt a proactive approach to brand protection using activities ranging from defensive registrations through to brand monitoring, in order to keep control of their brand and brand name in the digital world. How domain owners can monitor and prevent abuse of their domain name to protect themselves and their customers is clarified by Katrin Ohlmer from DOTZON.

Continuing with one of the worst instances of abuse on the Internet of abuse on the Internet, Alexandra Koch Skiba, Head of the eco Complaints Office, explains how the industry has been working together for the last 25 years, this year under the

motto of "Together for the Good of the Internet," to effectively deal with the removal of child sexual abuse material (CSAM), and prosecute perpetrators. Similarly, Els de Jong and Wido Potters from BIT take us through the development of SCARt, software that partially automates the processing of CSAM reports and the sending of NTDs (Notice to Takedown). Also on this topic, Kelly Hardy, Head of Registry Policy at CentralNic, deals with the challenges companies face not only in ensuring the takedown of illegal content such as hate speech and CSAM, but also in keeping their staff safe from all manner of revenge acts – including cyberstalking/bullying, threats, and hacking. For over 20 years, the international INHOPE network has been successfully working to combat depictions of the abuse of minors, says Peter-Paul Urlaub from the eco Complaints Office, giving an overview to the borderless fight against illegal content.

Finally, industry players can help to reduce abusive behavior by adding trust and security to the Internet through implementing and using current standards. Two examples: DNSSEC and DMARC. DNSSEC does two things: It ensures you're talking to the right online resource, and it verifies that the information you receive has not been tampered with, Patrick Koetter from sys4 AG explains. Together with Alex Brotman from Comcast, Patrick Koetter also points to how DMARC (Domain-based Message Authentication, Reporting, and Conformance) can help companies to protect their customers and their brands from abuse.

Of course, this overview is far from complete. But the greater the number and diversity of stakeholders that find their way to the table, the sooner and better the entire Internet industry can make a difference and make the Internet a better place. Consider this issue of dotmagazine as your personal invitation to join the conversation.

We wish you a great read and safe travels through the Internet!

Yours,  
 Thomas Rickert & Lars Steffen

# WHY PREVENTING, MITIGATING & FIGHTING ABUSE CONCERNS EVERYONE



Thomas Rickert, Director, eco Names & Numbers Forum, Attorney-at-Law, Rickert Rechtsanwalts-gesellschaft

**Thomas Rickert and Lars Steffen from the eco Association, on the importance of acting and collaborating in the fight against abuse involving the DNS.**

Can you imagine a world without the Internet? Probably not. It is the proven backbone of providing and sharing data, information, and services. Digitalization has probably already reached every aspect of our life. Very often the Internet is a mirror of reality. That means in turn that, very often, the Internet plays home to both the good and the bad. This is not a surprise. Given that the Internet is no longer new, the majority of the Internet industry is well prepared and active at preventing, mitigating, and fighting abusive activities online. However, what is new is the level of discussion and debate on abuse, as we currently see on DNS abuse.

For example, even though the Internet Corporation for Assigned Names and Numbers (ICANN) and its multi-stakeholder community have already been engaged in an extended dialogue on the topic of DNS abuse for over a decade, the topic of DNS abuse seems to be on everyone's mind these days. No ICANN meeting goes by without sessions on DNS abuse, while every industry event seems to put panel discussions and workshops on its agenda, and on 31 January the European Commission published its own study on DNS abuse. There are also working groups, teams, and committees among the different parts of the ICANN community and a number of industry driven initiatives, like the Internet & Jurisdiction Policy Network, the DNS abuse Institute by PIR, and eco's topDNS Initiative, that help to structure the discussion.



Lars Steffen, Director, eco International eco – Association of the Internet Industry

---

***The DNS is the foundation for the global expansion of the Internet as a universal public resource, but, like every innovation and every technology, they are facing abuse.***

---

This clearly shows many stakeholders have an interest in the stable, safe, and secure operation of the DNS. It has proven to be the foundation for the global expansion of the Internet as a universal public resource. However, like every innovation and every technology, the Internet and the DNS are facing abuse. Most involved stakeholders do not deny this either. But sometimes one can get the impression that very detailed interest-led discussions go round in circles regarding who should be responsible for doing what, and losing focus on the real issue. In these discussions some people are saying that the industry is not doing enough. And at the other end of the spectrum, you see people saying: well, actually, no, we are. The truth often lies in the middle – you need to be proportionate and reasonable in what you are asking others to do.

**Self-regulation – the importance of the industry seeking solutions to challenges**

By way of making the burden on Internet industry companies proportionate, at the eco Association, we work to support in their efforts to combat abuse. For more than 25 years, eco has been intrinsically motivated to make sure that abuse and illegal content are combated, and that crimes are prosecuted. Cooperating with the various stakeholders in the process is as important to us as neutrality and transparency. The eco Complaints Office, founding member of the INHOPE network, reports regularly on its experiences in combating illegal content online. Equally, since 2004 the Certified Senders Alliance has been a successful best-practice example of how email senders and

mailbox providers can collaborate in a self-regulatory trusted notifier framework to fight spam and phishing. Working groups dealing with the constant development of improved measures against abuse and projects to fight botnets within eco complete the broad portfolio of expertise within the association, and demonstrate the importance of these successful self-regulatory initiatives.

---

***It's always good for an industry to come up with ideas on how to respond to the challenges facing it with appropriate measures.***

---

Talking about self-regulation: Technical developments are, by their nature, by their dynamics, always faster than what legislators could ever achieve. Moreover, the Internet is borderless. It is a global tool that can be used by almost anyone around the world, whereas legislative initiatives by law makers usually have only national reach. If you are lucky, they have a regional reach, but there are almost no legislative initiatives that are binding on a global level. And that is why it's always good for an industry to come up with ideas on how to respond to the challenges facing it with appropriate measures. There is a risk of being held accountable for what your own users do. Then there is also the risk of legislators stepping in – perhaps with the best of intentions, but still intervening with legal instruments, laws, and regulations that go too far or have side effects that are detrimental to economic development and the use of technology.

---

***Tackling and preventing abuse on the Internet is complex and needs to avoid collateral damage to freedom and diversity of speech and over-blocking.***

---

Our goal is to bring all relevant stakeholders and intermediaries to the table and put up for discussion all different types of abuse that harm everyone on the Internet, to talk about roles and responsibilities across the board with the entire industry. The task of tackling and preventing abuse on the Internet is a complex one, one which needs to avoid collateral damage to freedom and diversity of speech and over-blocking. It's time to act and collaborate, not to point fingers at each other. It's time to give visibility to those who are engaged in the fight against abuse. It's time for sharing best practices with well-meaning players so that they can become better.



Source: © Istoma | iStockphoto

## **Making the Internet a nice neighborhood to do business**

In January 2020, Michele Neylon, long-standing eco member and CEO of Blacknight, a web hosting company based in Ireland, summarized perfectly why it is worth the effort to mitigate and fight abuse: "You know, you could live in the nicest neighborhood in whichever city or town you're living in. But you don't want to live in a neighborhood where there's rats bouncing across your front yard every morning, the bins are spilling out into the street, there's burnt-out cars at every corner. You don't want to live in that neighborhood. And why would anybody want to do business in that neighborhood? If you let the Internet's ecosystem degrade in that respect, then you end up in a situation where you end up going backwards. And that's not what we want – we want to move forward."

*Attorney-at-law and domain law expert Thomas Rickert is Director of the Names & Numbers Forum at eco – Association of the Internet Industry (international.eco.de).*

*Thomas Rickert is a member of the GNSO (Generic Names Supporting Organization) Council of the Internet Corporation for Assigned Names and Numbers (icann.org). Currently, At the beginning of 2022 he initiated the topDNS Initiative (topdns.eco) that unites members of the eco Association to fight DNS abuse. Further, Thomas Rickert is managing director of the law firm Rickert Rechtsanwaltsgesellschaft mbH (rickert.law), which is specialized in legal issues of the digital economy.*

*Lars Steffen is Director International at eco – Association of the Internet Industry (international.eco.de), the largest Internet industry association in Europe. At eco, he coordinates all international activities of the association and takes care of the members from the domain name industry.*

Read this article online at: <https://go.eco.de/mpZ3j1W>





# THE DEBATE AROUND DEFINING, PREVENTING AND MITIGATING DNS ABUSE



Simone Catania, Global Content & Communications Manager, InterNetX

**What is DNS abuse? Simone Catania from InterNetX looks at the definition of DNS abuse and describes scenarios for prevention and mitigation.**

DNS abuse is becoming an increasingly thorny issue for registries and registrars worldwide and ultimately for the global Internet audience. Solving DNS abuse or mitigating its effects requires a joint effort and some centralized functions and coordinated activities among the stakeholders. Recently, awareness around the topic appears to be growing and recommendations have been put forward.

DNS abuse is an important issue for the Internet ecosystem, one that requires more attention and urgent action. In this article, we want to introduce the topic of DNS abuse, outline the current problems concerning its definition and describe preventative and mitigating scenarios.

## The definition of DNS abuse requires globally recognized boundaries

One of the main problems in the DNS abuse debate originates from its very definition. As of today, a globally recognized definition of DNS abuse is lacking, as stated by ICANN, who also pointed out the urgency around this issue. Since there are no clear boundaries in DNS abuse, it is hard to define it accurately. A recent study on DNS abuse conducted by the European Commission has come up with this rather blurry definition:

"Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity."

So, what are these harmful or illegal activities that exploit the DNS? They include these five broad categories:

- Botnets
- Malware
- Pharming
- Phishing
- Spam (when used to spread other DNS security threats)

## Compromised vs. maliciously registered domain names

To define DNS abuse, it is important to make a clear distinction when discussing "abused" domain names. What seems to be internationally recognized is the differentiation between maliciously registered domain names and compromised domain names, the latter being domain names registered legitimately but subsequently taken over by cybercriminals.

### 1. Domains registered with the deliberate intention to harm

This is the first question we should ask ourselves. Is the domain registered maliciously? To answer this question, you could visit the website and see if valuable and trustworthy content is available. Then, check the WHOIS database. If the domain was registered only a few days before it got blacklisted, then a red flag should be going up.

### 2. Domains of hacked websites used to harm

Domain names might have been registered legitimately. The website gets compromised to serve illegal content and phishing campaigns. The legitimate domain names are usually registered many years before and the domain name is valid. A small percentage of abuse is perpetrated at the DNS level, such as domain shadowing attacks. The most substantial number of domains are abused at the website level because of vulnerable software like the Content Management System (CMS).

How can you distinguish between compromised domain names and maliciously registered domain names? There are two main approaches.

#### 1. Verification techniques carried out by humans

Individuals can verify a great deal of information related to the domain and draw conclusions. The age of the domain name and the time span between the registration and the blacklisting. Registrations carried out in bulk are also often a red flag. Techniques like cybersquatting, i.e., using a misspelled version of a brand name or service, are also relevant here.

#### 2. Verification techniques carried out through machine learning

Nowadays, there are many approaches based on machine learning. These were developed by different parties in order to achieve high accuracy in classifying domains based on publicly available data.

## Why is defining DNS abuse so complicated?

DNS abuse has different typologies and there is significant



Source: © MicrovOne | iStockphoto

overlap between different types of abuse. It acts in a large ecosystem composed of multiple public and private players (domain resellers, registrars, registries and hosting providers) that operate on a national, regional and international level to maintain the technical infrastructure of the DNS.

***There is an intrinsic difficulty in creating a clear division between technical security and content-related abuse. Too often, the boundary is neither clear nor straightforward.***

Furthermore, there is an intrinsic difficulty in creating a clear division between technical security and content-related abuse. Too often, the boundary is neither clear nor straightforward. For example, phishing attacks involve both malicious domain registrations and malicious website content. A piece of malware might exploit DNS vulnerabilities and spread harmful content on a website. At what level should DNS be fought and prevented? Who is in charge? These are two of the most crucial questions in the DNS abuse mitigation debate that we will try to answer.

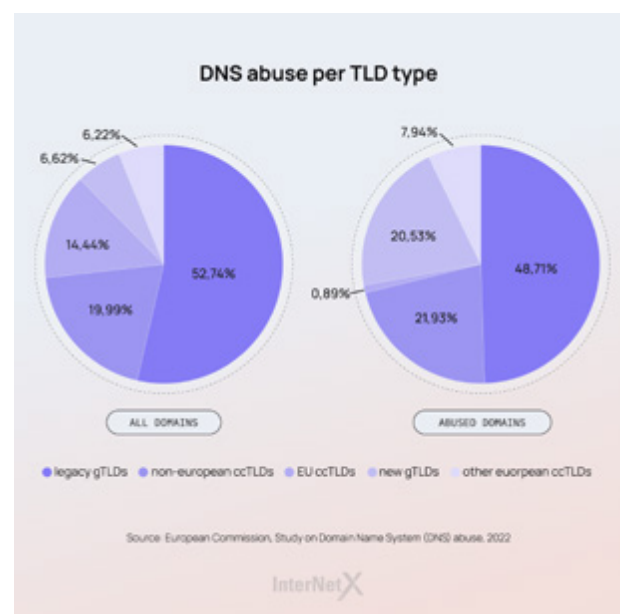
### An overview of DNS abuse in 2022

At the end of January 2022, the European Commission published a [report on DNS abuse](#). To assess the impact of DNS abuse, the authors conducted an overall health check of the top-level domain (TLD) ecosystems and different intermediaries such as domain registrars, hosting providers, and providers of free services. Concerning DNS abuse, the main findings from the report were:

1. In relative terms, the most abused TLDs are new gTLDs.
2. The two most abused new gTLDs account for 41% of all abused new gTLD domain names, which means that not all new gTLDs experience DNS abuse to the same extent.

3. European ccTLDs are the least abused domain names in absolute terms.
4. Most spam and botnet command-and-control domain names are maliciously registered. Legitimate users registered about 25% of phishing domain names and 41% of malware distribution domain names. They were compromised at the hosting level.
5. The top five most abused registrars account for 48% of all maliciously registered domain names.
6. The general adoption of **DNSSEC** remains low.

It is important to highlight that, for the first time, the EU has provided a helpful study that does not focus only on the "abused parties" but also on the intermediaries. The study proposes means of prevention, detection and mitigation of DNS abuse addressed



Source: European Commission, Study on Domain Name System (DNS) abuse, 2022

InterNetX

to DNS operators as well as international, national, and EU institutions and coordination bodies. Although the report shows some misleading analysis and inconsistent conclusions (as reported by CENTR), it does provide a clear signal that DNS abuse is being taken seriously and we can expect further development on this issue in the near future.

### Preventative or reactive DNS abuse mitigation?

Before implementing cost-driven measures and initiatives, the first thing you should do is identify a mitigation framework. The industry has implemented both reactive and preventative actions.

"Reactive initiatives" refers to all actions carried out by registries and registrars after receiving a report of abuse. It involves the investigation and mitigation of the threat once it has already been deployed. When undertaking reactive initiatives, your sphere of control only lies in improving the quality of the reports and the speed at which you react to warnings.

---

**Developing reactive responses to mitigate DNS abuse is absolutely indispensable - but so are preventative methods.**

---

Developing reactive responses to mitigate DNS abuse is absolutely indispensable. Still, we believe that focusing on preventative methods and detecting potentially malicious domains before registration is completed, or before the domain resolves, is the right course of action. No matter how quickly you catch a threat in a website or domain name, it was there already and the extent to which it affected users is unknown. You can only hope that the damage was negligible. Preventative measures are cost-efficient in the medium to long term and they certainly have a significantly more positive impact on business. But above all, they protect registrants from possible threats, since they are caught at an earlier stage, i.e. the threat is stopped before it reaches anyone.

### Where can you deploy preventative methods?

If you wish to carry out preventative measures to mitigate DNS abuse, one option is to analyze the domain name registration before the data is forwarded to the registry. Registries do not have much information about the registrant. Registrars are the intermediaries who collect most of the data.

---

**Nowadays, payment services providers offer fraud detection, and a suspicious payment authentication could be suspended altogether from registering a domain name.**

---

### Why is DNS abuse mitigation challenging to implement?

The problem with preventative measures is that they often cause friction in the registration process. In recent years,

registries and registrars have put a lot of effort into making domain registration easier. You need dedicated employees who write and integrate extensive and complicated code to carry out preventative measures. These actions bring no direct revenues to the players that make up the Internet ecosystem, which are primarily commercial entities. A real DNS abuse mitigation also needs to be sustainable for companies, or cost as close to nothing as possible.

### Who should mitigate DNS abuse?

There are three possible scenarios for identifying who could mitigate DNS abuse.

**Scenario 1:** Generally, the action needs to be taken at the DNS level for domains. Therefore, we need to consider the players involved in the registration process. If available, we start from the domain reseller and work back to the registrar and TLD registry.

**Scenario 2:** There are two different scenarios for malicious content. You start at the hosting level with the hosting reseller and hosting provider and then look at the DNS level for maliciously registered domain names. But when the domain name has been compromised, such as phishing content, you could start operating directly with the hosting operator.

**Scenario 3:** If the abuse concerns DNS operations, such as DDoS attacks against a DNS server, the measure needs to be addressed at the nameserver level.

### DNS abuse mitigation for a safer Internet

It should be clear now that the diverse Internet ecosystem makes it difficult to report abuse in any single meaningful way. Unfortunately, accomplishing the scope required has not been a core competency or primary goal for most organizations, including registrars and registries. Nevertheless, there have been more discussions around this issue from ICANN and other institutions recently.

There is certainly a long way to go before we are able to define clear paths forward, but we are confident that these are only first steps for much broader interest and global action.

*Simone Catania currently serves InterNetX as Global Content and Communications Manager. He is responsible for the content across InterNetX's blog and other channels and helps users understand the underpinning mechanisms behind the Internet. Simone is an ICANN fellow and member of EURALO and UASG.*

Read this article online at: <https://go.eco.de/QiDHZjr>

InterNetX



# DNS ABUSE: EVERYONE'S PROBLEM



Lars "LG" Forsberg, Chief Technology Officer, iQ

**Lars Forsberg from iQ looks at the need for awareness of DNS abuse, especially of the new gTLDs, because with awareness comes the ability to act.**

DNS abuse is a topic that is on the tip of the tongue for many. Questions on how to define, categorize, and report this menace have been discussed at all levels, which in turn has spawned frameworks, initiatives, and entire alliances. For the purposes of this article, I will be using the DNS abuse Framework definition of DNS abuse.

"DNS abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS abuse)"

Another popular discussion to consider on this topic is the one surrounding responsibility. Whose responsibility is it to be aware? Whose responsibility is it to act? In general, there is very little actual contractual responsibility in regard to DNS abuse.

The new gTLD agreement with ICANN includes a clause, Spec 11.3b, which requires the monitoring for threats, maintenance of reports on the number of security threats identified and the actions taken, and the report to be provided to ICANN if requested. However, Accredited Registrars are yet to be included in such a requirement and the discussion has not moved on very much in this respect.

---

***While there are currently no formal requirements, efforts are being made by community stakeholders to proactively minimize DNS abuse.***

---

But while there are currently no formal requirements, efforts are being made by community stakeholders to proactively minimize DNS abuse, one such example being the Quality Performance Index (QPI) from PIR, the Registry behind .org.



Source: © allanswart | iStockphoto

At iQ, when working to help customers with DNS abuse monitoring and mitigation, I consider the question of responsibility to be, if not irrelevant, then of less importance than the length of the discussion would indicate.

To make a lasting impact on malicious behavior such as DNS abuse, it is my strong belief that there needs to be awareness throughout the entire ecosystem. Everyone involved in the delivery of a service should know what is going on, should promote this, and should share information with our direct relations: Registries with Registrars, and Registrars with Resellers.

---

***With awareness comes the ability to act, and for each type of malicious action, there is an optimal, opposite, and equal mitigating reaction.***

---

With awareness comes the ability to act, and with a slight reference to the laws of nature, one could argue that for each type of malicious action, there is an optimal, opposite, and equal mitigating reaction.

This could, in and of itself, determine who should act, rather than a responsibility being handed out in a contract or, even worse, in national legislation where each country gets their own version of who should do what.

## How big is the problem?

The first step to awareness might not be to understand your own slice of the problem, but to grasp the bigger picture. So, how big is the problem and how is it trending?

Let's take a look at this using the Abuse Manager Threat Intelligence Feed. This data source is composed of meticulously monitored and vetted abuse reports, from well-known providers such as the Anti-Phishing Working Group and Spamhaus. The data source covers the same sources as the ICANN DAAR and several more.

On 2022-01-01, there were 2,108,649 reports of DNS abuse, regarding 1,113,820 domain names in the data source. One year prior, on 2021-01-01, there were 1,652,691 reports of DNS abuse,

regarding 793,291 domain names. That is an increase of 27.5%, in just one year. Each report falls under the definition of DNS abuse and each domain name is the smallest fully qualified domain name under the top-level domain name.

**Roughly one in every three hundred domain names is indicated in a DNS abuse report from a reputable threat intelligence feed.**

Today, roughly one in every three hundred domain names is indicated in a DNS abuse report from a reputable threat intelligence feed. Looking further into the data, the existence of reported DNS abuse is fairly consistent over top-level domain



names.

In 2021, 901 distinct TLDs were featured in reported DNS abuse. With roughly 1,500 top-level domain names in existence, this would indicate that only 60% of TLDs had any reported DNS abuse.

However, around 600 of the TLDs in existence are not available for registration, due to being a brand TLD or otherwise restricted. This means that the number of TLDs that are available for registration and have been featured in a DNS abuse report during 2021 is at, or close to, 100%.

The number of reports per TLD vary greatly, seemingly, due to price and popularity. Some TLDs, especially those with a high price, low popularity, or a small target market often see less reported DNS abuse than popular, low-cost domain names with a large target market. The relationship between \$1 campaign domain names and DNS abuse is real, but that is worth an entire article in its own right.

One thing that the graph above does not take into effect is the speed at which the malicious behavior is happening. During 2021, more than 16 million new DNS abuse reports were created, with an average of 45,000 reports per day.

The number of closed/removed reports is almost equal, standing at 44,000 reports per day. However, based on data gathered regarding these reports, and the domain name they regard, it would seem that only a small part of this is actually due to mitigation, with the overwhelming majority coming from the malicious actor moving on.

The average lifetime of a DNS abuse report is 32 days, with mitigating actions closing a report after an average of 7 days, based on iQ customer data. In comparison, the average time for a report to be closed due to the malicious behavior ceasing, without any detectable mitigation actions being taken, is 32 days.

**There is not a lack of DNS abuse reports to investigate, nor a lack of data on which to act, but there is a lack of awareness and a lack of action on the data available.**

In conclusion, I would say that there is not a lack of DNS abuse reports to investigate, nor a lack of data on which to act, but there is a lack of awareness and a lack of action on the data available.

**Is the pandemic a factor?**

A frequently asked question when it comes to DNS abuse is whether the ongoing pandemic has had an impact on these numbers. As noted, reported DNS abuse is increasing in general, and has been doing so for as long as iQ have been monitoring this data stream.

But, even so, the answer to this question would be yes. Some might be thinking of the initial reports of malicious behavior when it comes to the news cycle and products that attracted significant interest, but that was not the factor that accelerated things.

**The business case for malicious behavior became more appealing because of the pandemic propelling more people onto the Internet.**

Instead, the rate of growth in reported DNS abuse has been increasing during the pandemic due to the fact that more people are using the Internet for more things. The growth in reported DNS abuse is not related to the keyword pandemic, the facemasks, or to the vaccines.

It is related to new services, new behaviors and the increasing number of people using the Internet to do their work, to communicate with colleagues, and to live the life that would otherwise have happened out amongst people. The business case for malicious behavior became more appealing as a consequence of the pandemic propelling more people onto the Internet.





Source: © iQ

### What can be done?

Whenever someone asks me what can be done about DNS abuse in general, I always suggest the first step to be awareness. Get informed about the situation in general, and then get yourself informed about your own situation.

If you are struggling with finding information that relates to you and your company, I can recommend a free service called Abuse Stats. The service is provided by my company iQ, and is based on the same data source that I have used and referred to in this article. It can provide information on your current situation, and hopefully this will help you make an informed decision on your next steps. Whatever these steps may be, having a handy report delivered regularly to you, keeping you up to speed, is not a bad thing.

---

#### ***If you need to start thinking about how you mitigate DNS abuse, start by developing an Abuse Policy and an Abuse Management Process.***

---

If you are in a situation where you need to start thinking about how you mitigate DNS abuse, a situation in which most Internet-based service providers are, I recommend that you start by developing an Abuse Policy and a Abuse Management Process. The policy will make it easier to communicate up and down the line of services, and with end users that might be affected by your mitigation efforts. If you have to, or expect to need to scale your efforts, the process will be key to managing the work that you do.

Scaling is usually where most run into a problem. Investigating and mitigating DNS abuse is often manual and time-intensive work. A management system, be it a ticketing system or another tool useful for this purpose, is more or less essential.

Lastly, put your new policy and process to work. Take DNS abuse seriously, investigate the reports of malicious behavior thoroughly, and take action. Your policy should determine if an action you can take is the optimal course of mitigation, and if it's not, make sure that you share information with the party that could take this action, whoever this party may be.

If you want to get a head start and not have to "reinvent the wheel" yourselves, iQ offers a service called Abuse Manager. It's an easy-to-use SaaS platform that helps top-level domain registries, registry backends, registrars, resellers and other service providers that manage domain names receive accurate information about DNS abuse, as well as manage the work they do in mitigating the problem. My colleagues and I are also available to advise on matters such as developing a policy and process, or even managing your reported DNS abuse for you.

*Lars "LG" Forsberg is an industry veteran with more than 20 years of experience from the registry, registrar and service provider side of the domain name business. He has broad experience from roles held in development, operations and management, within organizations such as Loopia, the Swedish Internet Foundation (.se) and iQ.*

Read this article online at: <https://go.eco.de/7Y1pBA>



# CLEANING UP THE NEIGHBORHOOD



Source: © FelixRenaud | iStockphoto

**Michele Neylon, CEO of Blacknight, on illegal content, DNS blocking, and making the Internet a place people want to do business in.**

**dotmagazine: Michele, together with a set of companies you have produced a paper on DNS abuse. Could you tell me something about it?**

**Michele Neylon:** We're calling it the anti-abuse framework, or Framework to Address Abuse. There are about 50 signatories so far, including some of the biggest companies as both registrars and registries. In many respects, I suppose we're a bit of an anomaly, because we're a small registrar.

The framework is essentially saying that, as companies, we are willing to act on certain types of abuse without court orders. That if you report these to us, and we're able to verify the reports, we will take action. So here we're talking about things like the distribution of child sexual abuse material, the sale of illegal opioids, spreading malware, etc. These are things that, as companies in the infrastructure space, we can easily agree that we don't want to have. We don't want to be seen to be facilitating that kind of thing.

**dot: I can understand being interested in this kind of content from a hosting perspective, but where do DNS providers come into it?**

**Neylon:** There is a tendency to try and say that, as a registrar or as a registry or just providing DNS services, we are not involved in content. And I agree with and understand that argument. However, there is a line where it starts to become a little bit farcical. If you're made aware that something terrible is happening, and that a service or a product that your company is providing is helping to keep that accessible, then not taking action is a little bit ridiculous.

**dot: Is not taking action also a reputational risk?**

**Neylon:** Well, yeah, but it's not just reputation risk for us as

companies. I think it's also to do with the overall trust in the Internet ecosystem. The broader message around a lot of this is that, in order for the Internet to function and grow, for the digital economy to flourish, we obviously need to have various things in place. Obviously, you need to have decent infrastructure, you need to have decent broadband connections, you need to be able to take payments. There's a lot of these different things that come together. But fundamentally, underlying all of this is trust.

To put this in context: I didn't get a license to operate as a hosting provider. I went off and I got a couple of servers, started selling space on servers, and I grew from there. And if you look at a lot of the companies, perhaps the majority of the companies that are making waves in digital: we're not licensed in any respect. And that's perfectly fine, because the entire thing with the digital economy is that it's about permission in many respects. But the only way that works is if there is trust. And if you have a situation where everybody who goes online gets this perception that the Internet is full of bad things, and that they're going to have a bad experience, and there's all sorts of negative messaging around it, that destroys it for everybody.

---

***If you have a situation where everybody who goes online gets this perception that the Internet is full of bad things, and that they're going to have a bad experience, that destroys it for everybody***

---

So there is a certain degree of responsibility for actors within the ecosystem to keep it clean. Now, that does not mean that we become the Internet police. That does not mean that we are going to become the arbiters of what should or should not be on the Internet. But there are certain things where, unless you've got a very strange business model, you can pretty much agree that it shouldn't be allowed. I mean, child sexual abuse material is a simple one. It's a low-hanging fruit.

This does not mean that I'm going to go out and start policing my entire network and trying to find bad stuff on there. That's not what this is about. But if somebody sends us in a report of malware distribution, or some other kind of content that we can agree is illegal in some shape or form, then we're going to have a look at it, and if we feel it is appropriate, then we're going to do something about it.

**dot: Do you have a complaints procedure set up at Blacknight?**

**Neylon:** Of course. All registries and registrars that are



**Michele Neylon, CEO, Blacknight**

ICANN-accredited have obligations to have an abuse contact. And if you're a network operator, you should have an abuse contact as well. We're not a particularly large player, but we put that into part of our bigger help-desk system many years ago, so when something comes through, multiple people are able to access it. And then, depending on what type of complaint it is, we can deal with it immediately (for the low hanging fruit), but in other cases, obviously, it's going to be a lot more complex. We get complaints all the time, and you do get a lot of strange complaints. But the thing is just being able to look at them and decide whether it's within our scope to do something, or maybe we just pass it on to our clients, or in some cases it's simply not something that is within our scope.

**dot: Now, in the framework, there are a set of definitions of different types of abuse. Can you tell me something about this?**

**Neylon:** The thing to understand here is that the framework is very narrow and very specific and deals with a number of particular types of abuse. Like the child abuse example, which I keep using, because it's such a clear example. It's the one that there's really no grey areas about whatsoever, and there's no philosophical debate. It's black and white, it's binary. My own company will take action on quite a few other types of abuse. But, for example, if a website is compromised – which happens a lot – and we don't host the website, it would be disproportionate for us to take that website offline completely.

---

***As the registrar of records, but not hosting the website, the only action I could take is to remove the domain completely, which would be disproportionate.***

---

So let's say we are acting as the registrar of record for eco-member.de, for example. As the registrar of records, but

not hosting the website, the only action I could take is to remove the domain completely. I don't have a scalpel. I have no way of going in and saying these pages, these subdomains should or should not exist. I can't do that. And removing the domain completely would be disproportionate.

It's different if we are acting as the hosting provider – then it's sitting on our servers, we have access to the content, we have access to the files, and we can be much more refined in how to deal with it. If some things are sitting on a shared server, we can just take the web part offline. Their email, other services are not going to be impacted. Or we can even take just part of the website offline, or just make sure that's not accessible from the outside world. I mean, there's a lot of things that you can do.

But the thing is that a lot of this is coming from the bigger discussion around DNS abuse, because some people are saying that the industry isn't doing anything. And a lot of us are saying, well, actually, no, we are. There's plenty of things that we're doing. But you need to be reasonable in what you're asking us to do.

---

***There are certain things I can't do. For example, even if I'm the hosting provider, I have no way to remove a word from a web page. But we get people asking us to do this.***

---

There are certain things I can't do. I mean, for example, even if I'm the hosting provider, I have no way to remove a word from a web page. I can remove the entire website, but there's no way for me to go in and remove every definite article on a page. But we get people asking us to do this. And a lot of the time it's because either they don't understand how the ecosystem works, so they're sending the request to the wrong place, or they're just lazy – and don't make any real effort to contact the actual website operator. With something like defamation, for example, we get complaints, but the answer is: Go talk to our clients. They're in a position to do something about that. We are not. (Now sure, of course, if they were to present us with a court order demanding that we do it, fine.) But just assuming that because we're part of the chain we're able to do everything is not reasonable.

---

***The domain name, for example, it's just a pointer to the content. It isn't the content itself. But a lot of people seem to think that the domain is the content.***

---

If you look at the framework paper, it draws on some of the work from the Internet Jurisdiction Project. One of the things there is trying to explain to people how things fits together. The domain name, for example, it's just a pointer to the content. It

isn't the content itself. But a lot of people seem to think that the domain is the content, that they're one and the same. So if I remove eco-member.de, or .com or .whatever, all of the content you still have on that domain is still sitting there. It's still online, you just can't reach it through that domain.

So let's take Daily Stormer as a prime example. Daily Stormer keeps switching domain names, but the content is always the same. All they're doing is moving from one domain name to another. As the registries, registrars, DNS providers shut down those domains, they just switch. The content is always just there. It's just how you get to the content that changes.

---

**The document is dealing with very specific types of abuse. And if you talk to people in any of the companies signed on, in most cases they're willing to do a lot more. These are the minimum.**

---

**dot: Coming back to the framework: I assume you're wanting more DNS providers to become signatories?**

**Neylon:** Yeah. I mean, there are two parts to that. One thing is, obviously, you want more people to back these kind of base-line concepts. But the other thing is that there's no point in having, let's say, 500 companies sign on to this if 450 of them aren't actually going to do anything. You know, it needs to be meaningful. And again, if you look at the document, it's very narrow. It's dealing with very specific types of abuse. And if you talk to people in any of the companies signed on, you realize that in most cases they're willing to do a lot more. These are the minimum.

Essentially what you want is a situation where the digital economy can flourish and jobs can be created, and all of that. And I think these are all things that a lot of us believe in quite strongly.

---

**You don't want to live in a neighborhood where there's rats bouncing across your front yard every morning, there's burnt-out cars at every corner. And why would anybody want to do business there?**

---

But the only way that can work is if you're able to keep things relatively clean. I mean, you're never going to have a situation where the Internet is all unicorns and bunnies. That's just not reality.

You know, you could live in the nicest neighborhood in whichever city or town you're living in. But you don't want to live in a neighborhood where there's rats bouncing across your front yard every morning, the bins are spilling out into the street, there's burnt-out cars at every corner. You don't want to live in that neighborhood. And why would anybody want to do business in that neighborhood? If you let the Internet's ecosystem degrade in that respect, then you end up in a situation where you end up going backwards. And that's not what we want – we want to move forward.

*Michele is co-founder and CEO of Blacknight. He is actively involved in Internet policy development, and is currently a member of ICANN's GNSO Council as a representative of domain registrars. He is also involved with policy development for several domain registries, including .IE, .EU and .US. He previously served as chair of i2Coalition and is a member of the Names and Numbers Steering committee of eco. Michele received the Irish Internet Association Net Visionary Award in 2013 and was named one of Ireland's 30 Technology Disruptors at The Spiders Awards in 2019.*

Read this article online at: <https://go.eco.de/2qGnODL>





# GAINING MORE INSIGHT INTO MALICIOUS DOMAINS



Theo Geurts, GRC/privacy Officer, Realtime Register

**Theo Geurts from Realtime Register B.V. describes a proactive approach to malicious domains, based on analyzing and sharing data, and responding to incidents.**

Registrars have taken different approaches towards addressing malicious domains. Some remain more reactive, which means that their anti-abuse work is mostly focused on reviewing the reports of abuse that they receive. On the other hand, others have decided to be much more proactive and go beyond the mere receipt of the reports. One of the latter is Realtime Register, who have an Abuse Insight monitoring system that they put together over the course of several years.

## An effective anti-abuse implementation

In 2017, Realtime Register introduced an approach focused on incident response rather than on the receipt of reports. This approach provided them with detailed information on how cybercriminals operate (which they didn't have before, and which allows them to be much more effective in addressing abuse). However, it requires external tools and a process in which every abuse report that is received is strictly documented and analyzed.

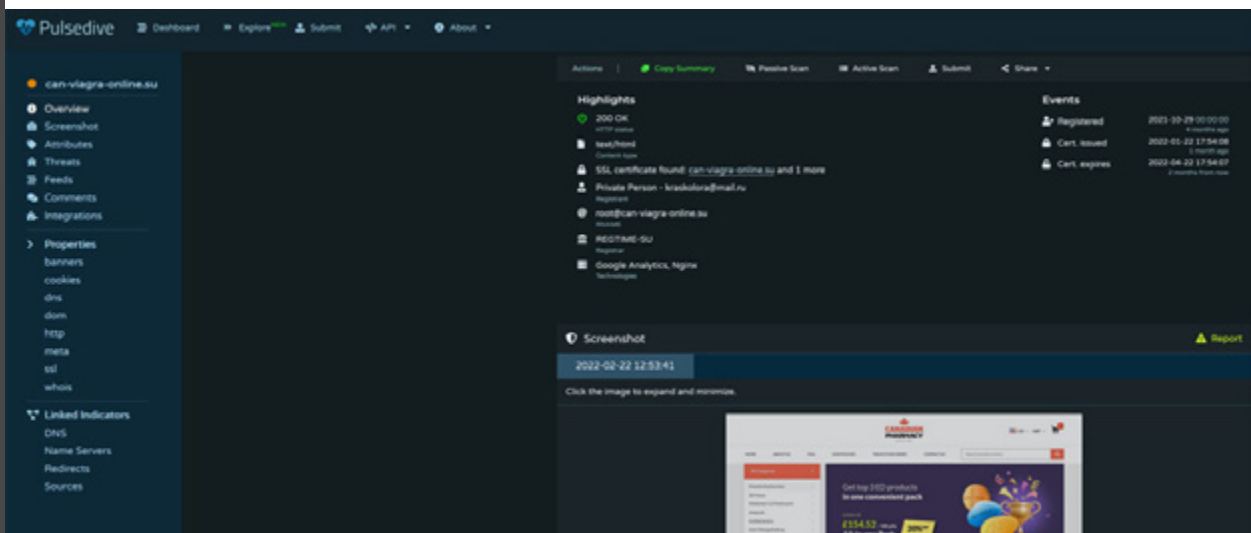
It's a combination of good data sources, sound systems, and an effective process. It was all built around five principles: Gather, analyze, share, exchange, and respond, referring to what can be done with threat intelligence in general and, in particular, regarding malicious domains: Gather data from high quality domain reputation feeds, use good analysis tools that allow detailed correlations (visualizations are a great plus), share with registries, resellers and other parties who can act on the information to mitigate the threats, exchange information with those who may have related information that is of interest, and respond by acting on the actionable information in order to mitigate the threats.

## Reseller access to a visual dashboard

Realtime Register currently use Microsoft's Power BI, which provides visualizations, has some nice analysis features, and is also a platform to create dashboards. And the dashboard is available not only to Realtime Register: Very importantly, they make it freely available to their resellers. It was the cheapest option for their existing settings, making it the easiest solution to then get started with.

## In the dashboard, resellers can:

- See data like abuse percentages for their domain portfolio calculated based on PulseDive.com abuse data, rescanner domains, and see the source of malicious activity. Each reseller can see the ratios per abuse type within their portfolio, so they know that they have X% of malware domains, Y% of phishing domains, and so on.
- Resellers can zoom in on one given indicator or domain and see more details. Also, they can see the source reputation feed that lists the domain and the kind of activity that it was listed under.



The screenshot shows the Pulsedive dashboard interface. On the left, there's a navigation menu with options like Overview, Screenshot, Attributes, Threats, Feeds, Comments, Integrations, Properties (banners, cookies, dns, ipam, http, meta, ssl, whois), and Linked Indicators (DNS, Name Servers, Redirects, Sources). The main content area displays a 'Virus Summary' for the domain 'can-viagra-online.su'. It includes a 'Highlights' section with items like '200 OK', 'SSL certificate found', and 'Private Person'. There's also an 'Events' table with columns for event type and date. A 'Screenshot' section shows a thumbnail of the website with a 'Report' button. The website screenshot shows a page with a 'Get top 100 products in one convenient pack' offer for £254.92.





- When zooming in on a particular domain, they can see the subdomains and URLs associated with it, which provide even more information about the abuse.
- Resellers can then zoom in once again, this time on the particular feed itself that provided the listing, where they will find all the specific details of the abuse with the corresponding analysis and all other available data.
- The data from Pulsedive goes back to 2018 and provides historical context to the resellers.
- Zoom in on other reputation blocklists available (75+)

The dashboard is updated every 24 hours. For all feeds (except some that are updated every hour), Realtime Register additionally sends a notification of abuse report events through an API or via email to the corresponding resellers (often hosting companies).

According to their analysis, since 2018, the average abuse percentage of DNS abuse at Realtime Register is 0.03%. They intend to continue using their systems and process to keep it well under control.

### Predictive analysis

To stay ahead of the game, a system has been set up that runs in the background and reviews each newly-registered domain name to check metadata, assign a scoring, and generate a daily report indicating which domains may become malicious and may warrant extra investigation. When a domain is included in this report, the next step is to check whether the registrant data is bogus or corresponds to an already-known malicious registrant and whether the domain is associated with other data points already known to be related to malicious activity (like IP addresses, name servers, and others)

It still requires human review because there still are false positives, but it works. It lets us see what's coming and stop it before it does any harm, like in banking phishing.

### Conclusion: Commercial benefit

DNS abuse raises costs for registrars who have to do all this anti-abuse work. Margins are thin, but abuse prevention results in lower costs, and resellers are in a position to claw back some of those costs. Certain registries also factor in abuse levels in calculating discounts and promotions for registrars, which are sought after because they provide better margins.

Also, by being proactive and suspending domains in advance of them being used, they ensure that they don't get reports of abuse, which are expensive to deal with.

In other words:

- Preventing the creation of malicious domains means reduced costs associated with the anti-abuse work required to deal with malicious domains.
- Properly addressing the malicious domains that do get created can result in discounts from the registries to the registrars, which could help their sales increase with even higher margins.

So, there is commercial sense in a registrar doing anti-abuse work. It is not just a dead cost, a burden. In the case of Realtime Register, they keep their good reputation, they probably are treated very well with discounts by the registries who also benefit from cleaner TLDs, their resellers stay clean, and the global Internet benefits from a cleaner domain name industry.

This is an example that other registrars could follow. Effective anti-abuse work that brings commercial benefits. Why not?

```

File Edit View Search Terminal Help
>> Progress: 74.9 %

[*] Verifying keyword: dhsbank [ 136 / 180 ]
>> Progress: 75.1 %
>> Progress: 75.3 %
>> Progress: 75.5 %

[*] Verifying keyword: lngbank [ 137 / 180 ]
>> Progress: 75.7 %
[*] Similarity detected between lngbank and lngbank.lnk (high confidence)
>> Progress: 75.9 %
>> Progress: 76.1 %

[*] Verifying keyword: smsbank [ 138 / 180 ]
>> Progress: 76.3 %
>> Progress: 76.5 %

[*] Verifying keyword: trilodes [ 139 / 180 ]
>> Progress: 76.7 %
>> Progress: 76.9 %
>> Progress: 77.1 %

[*] Verifying keyword: scottlabank [ 140 / 180 ]
>> Progress: 77.3 %
>> Progress: 77.5 %
[*] Similarity detected between scottlabank and scottlabank.cloud (very high confidence)
>> Progress: 77.6 %

[*] Verifying keyword: abnanro [ 141 / 180 ]
>> Progress: 77.8 %
>> Progress: 78.0 %
>> Progress: 78.2 %

[*] Verifying keyword: argenta [ 142 / 180 ]
>> Progress: 78.4 %
>> Progress: 78.6 %
>> Progress: 78.8 %

[*] Verifying keyword: tangerine [ 143 / 180 ]
>> Progress: 79.0 %
>> Progress: 79.2 %
[*] Found shoptangerineboutique.com
[*] Found tangerineflorida.com
>> Progress: 79.4 %

[*] Verifying keyword: fedex [ 144 / 180 ]
[*] Found 8urs1-fedex.com
[*] Found 2b1fe-fedex.us
[*] Found 1qfuf-fedex.com
[*] Found 1r93y-fedex.us
[*] Found 2b187-fedex.us
[*] Found 2vb6y-fedex.us
[*] Found 2hcn1-fedex.us
[*] Found 2289t-fedex.com
[*] Found 8v1cf-fedex.us
  
```

Theo Geurts has worked within the DNS industry for over a decade and contributed to many of ICANN's policies. For the last four years, Theo's focus has been on Cyber Security, OSINT, and ethical hacking. He played an essential role in DNS abuse investigations ranging from BEC fraud to cyber terrorism.

Read this article online at: <https://go.eco.de/CdznK3k>



# QPI: A “CALL TO ARMS” ON RESPONSIBLE GROWTH



Source: © Natali\_Mis | iStockphoto

**Inma Del Rosal Mendez and Brian Cimboric from PIR explain how the Quality Performance Index supports a reduction in abusive domain registrations.**

Public Interest Registry (PIR) is the nonprofit registry operator of .ORG and several other mission-driven gTLDs. As part of our nonprofit mission, we strive to be an exemplary registry, and develop best practices not just for .ORG, but for the broader Domain Name System (DNS).

One of PIR's cornerstone initiatives is called QPI, or the **Quality Performance Index**. Launched in 2019, QPI is a PIR channel program that incentivizes registrars that promote and maintain healthy domain registration patterns (e.g., low abuse rates) by providing discounts on the price of .ORG registrations. QPI seeks to promote a healthy .ORG domain space that focuses on creating responsible .ORG registrations while implementing proactive steps to reduce DNS abuse.

Since the launch of the QPI, we have gained some remarkable insights. First, a proactive abuse approach is good for business, reflected by a significant improvement in renewal rates for both PIR and for those registrars who are eligible and participate in QPI. Second, creating an environment where abuse is less likely to occur results in much less abuse mitigation for registries and registrars.

---

***A proactive abuse approach is good for business, reflected by a significant improvement in renewal rates for both PIR and eligible registrars.***

---

These outcomes could have a significant impact on the Internet ecosystem, and we are keen to share them with the

industry. We invite domain name registries to review the QPI program and its associated benefits. PIR developed QPI so that it can be adapted to fit the needs of individual registries, and we are dedicated to making sure other registries have the tools they need to develop and implement their own version of QPI. Our goal is to encourage more registries (and potentially wholesale registrars) to adopt their own QPI as part of a greater, more global effort to tackle abuse across the DNS. We believe that registries doing so will see the benefits of responsible growth coupled with lower abuse rates.

## **Developing and implementing QPI**

QPI is based on several key performance indicators: abuse relative to new creates, renewal rates, domain usage, SSL usage, DNSSEC enablement, and average term length (ATL). We thank our friends at **SIDN, the ccTLD registry operator for .NL**, who helped us brainstorm and discuss QPI, since SIDN previously launched its “Registrar Scorecard,” which also focused on registration quality.

---

***As a registrar's QPI score goes up, it qualifies for higher tiers of discounts.***

---

QPI is calculated by analyzing data for each registrar based on the six metrics noted above. The weighted scores are then combined to form a single QPI score. If the QPI score meets or exceeds the baseline threshold established by PIR, the registrar is then qualified to participate in the promotion pending any additional terms and conditions requirements. As a registrar's QPI score goes up, it qualifies for higher tiers of discounts.

---

***Our channel incentive programs are designed to reward registrars with low abuse relative to their size.***

---



**Inma del Rosal Mendez, Senior Director Channel Services, PIR (Public Interest Registry)**

While we have fine-tuned these metrics over the last three years, the most heavily weighted metric is abuse rates. If a registrar fails the abuse rate metric, it is ineligible to participate in QPI even if it achieves a perfect score in every other QPI category. Our channel incentive programs are designed to reward registrars with low abuse relative to their size. We will continue to evolve and improve QPI over the years but what will not change is our commitment to quality growth and to combating DNS abuse.

### Reduction in abuse

.ORG has been and remains the least abused of all large gTLDs. Since implementing QPI, we have seen .ORG's abuse decrease significantly.

Spamhaus is a third-party watchdog organization that both maintains reputation blocklists and also publishes a "badness" score for all TLDs. Prior to implementing QPI in 2018, .ORG averaged a 4.1% "bad domains" score according to Spamhaus, which (even at the time) was the lowest of all "legacy" gTLDs.

Since implementing QPI, .ORG's badness score decreased to 3.4% in 2019, 2.16% in 2020, and 1.59% in 2021. In comparison, the other legacy gTLDs averaged anywhere between 4.68% to 16.67% bad domain scores in 2021.

---

***Registrars that had previously had unacceptably high abuse rates have worked to lower their abuse percentages to qualify for QPI and gain the associated financial incentives.***

---

QPI is both a "carrot" in that it provides financial benefits to registrars with healthy registrations, and a "stick" in that lower performing registrars know they are not receiving the financial benefits of some of their competitors with more robust anti-abuse practices. PIR has observed direct changes in some registrar behavior; registrars that had previously had unacceptably high abuse rates have worked to lower their abuse percentages in order to qualify for QPI and gain the associated financial incentives.



**Brian Cimboric, Vice President, General Counsel, PIR (Public Interest Registry)**

### Increase in business

One of our goals is to responsibly grow .ORG Domains Under Management (DUM) and to offer attractive promotions to our channel. However, we also strive to maintain a quality namespace with minimal abuse rates. QPI enables us to strike this balance and we are very pleased with the results. Abuse rates are down year-over-year and we have seen an increase in sales for participating registrars.

We're now at the point where nearly 60% of all .ORG new creates flow through the QPI program. Prior to launching QPI, .ORG had approximately 10.1M DUM. Despite our focus on quality over quantity, .ORG DUM currently sits at approximately 10.7M. When we launched QPI in 2019, our renewal rates were 77.4%. Now, after several years of focusing on quality registrations through QPI, our renewal rate has grown to 82.3%, the highest for all large gTLDs. We know that quality registrations are much "stickier" and a domain that renews is much less likely to engage in future abuse.

---

***The QPI program is contributing to growing .ORG responsibly by focusing on quality registrations.***

---

We have seen results in the QPI key performance indicators. Registrars that participate in QPI gain a 4% improvement in their own renewal rates for .ORG, an increase of 1.6% in usage (developed domains), a 44% increase in DNSSEC enabled domains, a 9.9% increase in SSL active domains, and a 0.1% increase in ATL (Average Term Life).

These statistics demonstrate that the QPI program works and is contributing to growing .ORG responsibly by focusing on quality registrations. We continue to see domains renew, and renewals ultimately bring recurring revenue.



Our registrars have acknowledged the benefits of the QPI as well. For example, Uli Retzlaff, a domain expert at IONOS, notes: "IONOS relies on quality registrations to drive global growth in the hosting and cloud business. As a result, PIR's initiative to analyze, forecast and incentivize domain registrations that lead to higher renewal rates and greater customer perceived value just makes the work we do easier and more profitable. We're very grateful that PIR's QPI program aims at growing the value of .org domains in particular, especially because speculative, short-lived registrations are not key to our business model at IONOS."

Karen Dixon, VP of Marketing Domains at Newfold Digital (formerly Endurance Group), notes: "We've been really pleased to participate in the QPI program and have found a lot of success with it throughout the year. It's helped to incentivize us to find more opportunities to sell .ORG domains across our organization and has resulted in a more than 50% increase in creates YOY. We love to see registries come up with creative programs that reward registrars who are focused on selling quality registrations – it's a win-win for us both."

And Ashley Barton, Senior Director of marketing at Name.com, says: "PIR has been a key partner for Name.com over the past few years thanks to the QPI program, which incentivizes and rewards us for driving long-term, sustainable growth. Rather than chasing volume on low cost, first-year registrations, we can leverage the QPI program in alignment with our broader strategy of driving quality registrations with higher renewal rates. This focus on long-term success over short-term volume has led to an increase in .ORG revenue, which benefits both registry and registrar."

Ultimately, PIR wants to assist our channel to better understand QPI. We can help our registrars to improve their scores, to ensure participation in future programs, and to help grow their business. As an evolving initiative, we gather and implement registrars' feedback with the goal of enhancing the results of the QPI. We are always happy to welcome additional feedback from our channel partners.

**QPI Toolkit: Arming registries with tools to develop their own QPI**

In order to advance our goals of quality growth and to reduce DNS abuse, we published a QPI Toolkit that any registry can utilize. The QPI Toolkit includes a framework for QPI adoption and a formula spreadsheet that can enable other registries to implement their own QPI scoring. PIR understands that other registries and wholesale registrars can adopt QPI principles in a manner that works best for them. We are also happy to speak with any registry or registrar about QPI or how to develop a system like QPI. Each registry and wholesale registrar that deploys a QPI-like system will have slightly different approaches, which

is totally understandable, but if more of them adopt a philosophy that tries to grow responsibly, we believe it will make a significant positive impact on DNS abuse.

**PIR's other anti-abuse initiatives**

In 2021, we created the DNS abuse Institute which develops tools to help mitigate DNS abuse and create best practices for registries and registrars to effectively combat abuse. We're also proud to serve on the eco's topDNS Steering Committee and collaborate with other industry leaders to develop solutions to combat abuse.

*As Senior Director of Channel Services at Public Interest Registry (PIR), Inma del Rosal Mendez is responsible for overseeing the global growth of the registry's product portfolio, which includes the .ORG family of domains (.ORG, .NGO, .ONG, .FOUNDATION, .GIVES, .CHARITY, and other mission-driven TLDs). She leads a diverse global team responsible for developing integrated channel strategies and nurturing relationships with registrars, resellers, and other partner organizations. Inma has more than 14 years' experience in the domain industry, having worked on the account management team at Verisign prior to joining PIR. Inma lives in Switzerland and holds a Master Degree in Law from UNED University in Spain.*

*Brian Cimboric is the General Counsel for Public Interest Registry (the non-profit registry operator for .ORG) and oversees its legal affairs and Anti-Abuse Program. Brian serves on the topDNS Steering Committee and is also Coordinator of the Internet and Jurisdiction Policy Network's Domains and Jurisdiction Program. Brian was one of the co-creators of the Framework to Address Abuse and one of its primary authors. Brian also serves as Co-Chair of the Registries Stakeholder Group DNS abuse Working Group.*

Read this article online at: <https://go.eco.de/pbS4u7k>





# NOT IN OUR DOMAIN: HOW EURID IS USING AI AND GLOBAL COOPERATION TO TACKLE CYBERCRIME



Alastair Gill, Journalist and Editor

**EURid takes an innovative approach to help out-wit cybercriminals, including helping to identify potentially malicious registrations at source.**

Domain names are a key link in the chain that facilitates abusive online activity. If cybercriminals are able to register a domain name, they have a platform from which to target their victims, whether via phishing, spam, botnets, or malware.

Fighting domain name abuse is a constant challenge for EURid, whose .eu is an attractive domain for ambitious businesses looking to reach other markets and secure future growth: the .eu top-level domain represents 30 countries (EU and EEA member states), EEA citizens around the world, and around 450 million people with one clear extension. A tempting opportunity for cybercriminals.

***The Abuse Prevention and Early Warning System (APEWS) analyzes domain registrations & delays potentially abusive ones – before they can be used to carry out any attacks.***

EURid's answer is the Abuse Prevention and Early Warning System (APEWS), a groundbreaking solution that uses AI and professionally curated incident lists to analyze domain name registrations and delay potentially abusive ones – catching them before they can be used to carry out any attacks. EURid began working on the project in cooperation with KU Leuven in 2017, and APEWS finally went online in December 2019.

## **APEWS vs. abuse**

If the APEWS system flags a domain name registration as possibly linked to misuse, it is placed on hold pending further verification before it is delegated to the .eu zone file. This means that any services attached to the domain name (such as a

website or email) will not function until the registrant's identity has been fully corroborated.

***Any services attached to the domain name (such as a website or email) will not function until the registrant's identity has been fully corroborated.***

"If we detect that a domain which has been registered shares some similarities with something that was abusive in the past, we ask the registrant about their identity – are you really the person that you say you are? Could you please identify yourself?" says Jordi Iparraguirre, Innovation Manager at EURid.

Suspicious cases are not only reviewed by EURid itself – the organisation also shares details of the registration with cybersecurity experts and law-enforcement bodies like Europol. But what makes a registration suspicious?

"We're not just looking at the domain name itself," explains Iparraguirre, whose role at EURid is to lead the development of new products and services so as to better serve .eu users. "We're looking at lots of metadata around that domain. The system is fed with lists of domains that, for instance, have been used for spam or phishing in the past."

This kind of historical data helps the system to tag a registration as potentially abusive – even if the domain is not the same as a previous offender. In most cases, further checks are necessary, says Iparraguirre, but "when you see sites that are selling counterfeit products, you can be almost certain. Or a clone of a bank webpage – we've seen that – or the tax office, then that's clear."

***EURid is setting up systems so registrants can self-validate their identification using eIDAS (a European-wide system for electronic identification) or a credit card.***

Some cybercriminals make amateurish attempts to prove their identity by submitting expired ID cards or retouching dates and information – "We've seen masters of Photoshop sending very interesting 'proof'," says Iparraguirre – but the people behind most suspicious registrations disappear and the registrations are subsequently suspended.

EURid is setting up systems so registrants can self-validate their identification using eIDAS (a European-wide system for



Source: © metamorworks | iStockphoto

electronic identification) or a credit card, as well as other methods. EURid does not keep personal data, it simply checks whether the registrant's identity has been validated by these trusted ID schemes.

**Change is the challenge**

---

***While APEWS is capable of self-training, the system still requires input when cybercriminals suddenly alter their approach.***

---

According to Sameh Mannai, a data scientist and AI software developer at EURid, APEWS has shown excellent performance in detecting malicious campaigns – 80% recall (the proportion of actual positive labels correctly identified by the model) and 80% precision – but while it is capable of self-training, the system still requires input when cybercriminals suddenly alter their approach – as they often do.

"The main challenge is that the behavior of abusers is continually changing, and the data is different, the performance of APEWS will naturally degrade over time, and we have to feed the system with new data so that it can recover and improve its performance," she explains.

"It needs to be constantly updated with new training data to remain accurate over time, but this is the case for most machine learning models. And this is what APEWS does: it automatically retrains regularly to catch up with these changes."

Global events such as Covid-19 are a gift to abusers as they are usually impossible to predict, making it essential for cybersecurity bodies to react quickly to new threats. The coronavirus outbreak in 2020 and the ensuing global pandemic saw an

explosion in fraudulent online activity as cybercriminals around the world seized upon the health crisis to exploit people's fears by selling them fake tests, certificates, masks or sanitizers.

In response, EURid updated APEWS to protect end-users from potential misuse of domain names by programming it to perform additional checks if newly registered domain names contained keywords related to the pandemic.

**Educating the younger generation**

Beyond its own in-house projects, EURid collaborates actively with a number of other organizations on initiatives to combat online abuse. One is the Youth IGF, created and administered by TaC-Together against Cybercrime International, a global non-profit anti-cybercrime organization based in Geneva and Paris. The main goal of the Youth IGF, which has been the leading youth movement on Internet governance since 2011, is to help victims of Internet crime and develop educational tools on online safety and cybersecurity for various stakeholder groups.

---

***"At the beginning of the pandemic, we launched CyberVictim.Help because cases were rising and there was a need to provide victims with an immediate response."***

---

"As one of the partners of the Youth IGF, EURid is helping the Youth IGF to bring the voice of youth on the digital world to policy makers," explains TaC founder and director Yuliya Morenets. "Cybersecurity is a strong focus of the Youth IGF's work."

By supporting the Youth IGF, EURid contributed to the implementation of innovative solutions like CyberVictim.Help, which provides victims of cybercrime with assistance.

"At the beginning of the pandemic, we launched CyberVictim.

Help because cases were rising and there was a need to provide victims with an immediate response. Our trained Youth IGF Ambassadors made this real-time assistance possible, as they are located in different time zones and different linguistic regions.”

### Protecting brands from abuse

When it comes to abuse prevention, businesses can also reduce risk by protecting their intellectual property rights at the European Union Intellectual Property Office (EUIPO).

EURid has collaborated closely with the EUIPO for several years and, in 2020, it strengthened its efforts by helping users of the EU IP system to obtain trademark and domain name protection so that their brands are secure.

“We’re well aware of the risks entrepreneurs encounter when they launch and run their businesses,” says Ingrid Elisabeth Buffolo, Director of EUIPO’s Customer Department.

“Here at the EUIPO, we are fully committed to supporting EU business. For example, when a company registers a European trademark, the applicant can immediately access information in order to understand whether an identical or similar .eu domain name is already registered. Offering this information to a European trademark applicant will facilitate the registration of the company’s .eu domain name, avoiding cybersquatting or domain name abuse.”

### An AI on the future

EURid is also working on a number of other applications of AI technology. It is developing automatic multilingual web page classification, and has implemented a system that offers new registrants a choice of alternative available domain names if the one they want is already registered.

Cybercriminals may be constantly improving their tactics, but EURid is showing that, through the intelligent use of innovation and strategic alliances, it is possible to stay one step ahead in the game.

*Alastair Gill is a British journalist and editor focusing on geopolitics, culture and technology.*

Read this article online at: <https://go.eco.de/4MJDaGb>

**EURid**



# EMAIL BLOCKLISTS FOR REAL-TIME DETECTION AND MITIGATION



Source: © Natali\_Mis | iStockphoto

**Patrick Ben Koetter from eco Email & Anti-Abuse Competence Groups speaks to Lars Steffen from eco about blocklists, allowlists & the value of reputation.**

Email is a zero-tolerance medium, explains Patrick Ben Koetter, Board Member of sys4 AG and Leader of the eco Email and Anti-Abuse Competence Groups. In interview with eco International's Lars Steffen, he provides insights into the recently published advice for mail server administrators on selecting suitable blocklists, developed by the eco Email Competence Group, and discusses the increasing importance of IP reputation for the successful delivery of commercial emails.

**Lars Steffen: Patrick, you have recently been involved in updating the eco Email Competence Group white paper on blocklists. What have been the big changes?**

**Patrick Ben Koetter:** Firstly, there has been a change in terminology, moving away from blacklist and whitelist to blocklist and allowlist. It doesn't hurt us to do this, and it does others good. This terminology issue was beginning to emerge at the M3AAWG meeting in Canada the year before last. So we took the opportunity to change our usage in the updated paper.

Apart from that, we sharpened some terminology that we thought was needed. The basic message of the paper – that email blocklists exist, that they are useful, and how to ideally choose a good list – still remains in the new version. What has also remained is the basic message about why we might reject a particular list because we don't think it's appropriate. The basic finding is that some lists we had hoped would improve over time have unfortunately not improved. We continue to believe that there are a few list operators that simply should not be used.

**Steffen: What are the reasons for not including or for criticizing certain list operators?**

---

***Great care needs to be taken with implementing filters to avoid the possibility of these filters being hypercritical.***

---

**Koetter:** Email is a zero-tolerance medium. Everyone thinks email is kind of stupid, but if it doesn't work for a second, everyone thinks it's even stupider. For that reason, great care needs to be taken by anyone who implements filters to try to let through only the stuff that an email recipient wants. You want to avoid the possibility of these filters being hypercritical and filtering out things that shouldn't be filtered out. When this

happens, you want to be able to turn that off as quickly as possible. This is where the wheat is separated from the chaff in terms of good and bad blocklists.

Blocklists are decidedly practical. They are created by having sensors all over the world that perceive whether someone is sending spam or not. These blocklists are updated to provide real-time information about which computers you should avoid communicating with because they might be sending spam.

---

***If someone is mistakenly put on a blocklist, then there needs to be an effective and efficient delisting process. If this does not exist, then this is a list you should not use.***

---

At the same time, if someone is mistakenly put on such a list, then there needs to be an effective and efficient delisting process. If this does not exist, then this is a list you should not use. So one reason not to use a list would be, for example, if there is no explanation of how to get off this list again. Another reason would be that the people who edit this list may only edit it periodically, and therefore it may not be acted upon quickly enough.

And an even more important reason would be if someone says: If you want to get off this list right now, you have to pay us money. Such providers exist, and we do not recommend using them, as there is a conflict of interest in this case. One might assume that the operators are not interested in updating the list quickly. And that they have an interest in listing everyone in the world if possible, because then everyone in the world will want to pay money to get off the list. The suspicion here is that this is their business model, and that's not on. You have to stay extremely far away from such things.

**Steffen: Has the need for blocklists increased in recent years?**

**Koetter:** For basic understanding: Depending on which statistics you look at, between 97 and 99.9 percent of all emails sent around the world are spam. This raises two problems. First: I want to filter out the spam. And secondly, if you think about how much load this generates: I want to take as much load off the servers that have to process the spam as possible. So, on the one hand, there is this huge amount of spam, and, on the other hand, there's an insanely large load on the mail servers that have to filter it out. So you want to find out as quickly as possible whether you want to talk to the computer that is currently connecting to you or not. And the best means of choice to decide this are simply IP-based blocklists. You can look at these lists and say: I know the IP, it's on the list. I don't want to talk to you. For this reason, blocklists still have their justification.

---

***IPv6 turns the principle around and goes over to so-called allowlists.***

---

Now, fortunately, there is an increase in the use of IPv6 on the Internet. The number space in IPv6 is so much larger than in the IPv4 network, meaning that it is not possible to build blocklists that would block all these machines and IP addresses. No one can put that many hard drives anywhere. This is why blocklists for IPv6 are not a means of choice. You can't write one big enough. That's why IPv6 turns the principle around and goes over to so-called allowlists. Here, the logic is: I know this IP address and I know that it has a good reputation by now, so I allow it to send to me. Will there be a lot of use of IPv6? Yes, hopefully. Is this already happening today? Not really yet. That's why we'll be dealing with IPv4-based mail servers for a very long time to come. And for this reason, we will continue to need IPv4-based blocklists for quite a long time.

**Steffen: You mentioned updates to provide real-time information. Is this really necessary or just a nice-to-have?**

---

***Many malware campaigns we see pop up somewhere for 10 minutes, cause a lot of damage, and disappear.***

---

**Koetter:** Spam and ransomware attacks are passed on insanely fast. Abuse cases that we have today spread rapidly on the net and disappear again. Many malware campaigns we see pop up somewhere for 10 minutes, cause a lot of damage, and disappear. Reactions need to be quick – because within 10 minutes, the damage has already been done. Ideally, you will have already noticed with the help of a blocklist that you do not want to communicate with the affected computers and will have reacted accordingly. Which is why it's increasingly important that we have real-time lists that can be queried instantly. And that includes being able to query lists easily and in fractions of a second. I know from my experience with Abusix that, on average, there is about a second between a honeypot registering something and the entry going on the blocklist.

**Steffen: And how quickly does the information reach those who use the list?**

**Koetter:** That's the interesting point. This is covered in our paper. From a purely legal point of view, it is quite questionable to use a mail server that is located in Germany to query a service that is not on your platform. Because it means that you pass on an IP address of a device to a third party, and an IP address is definitely something that can be considered as personal data from the point of view of data protectionists. So if you query a service in America with your mail server, they learn a lot about our communication habits. This is a difficult issue from a data



protection perspective. That's why the big providers have developed processes that copy the data from the supplier over to their own platform as quickly as possible and use it there.

---

***Reputation-based systems mean that the significance of an IP address is nowhere near as important today as it once was in determining whether to accept an email.***

---

However, these procedures are no longer fast enough. You have to be able to query the data live because a lot happens in just one minute. This is why, in addition to what can be achieved with blocklists, people have also started to create so-called reputation-based systems. This means that the significance of an IP address is nowhere near as important today as it once was in determining the overall impression of whether to accept an email. In the past, a mail server was configured to check whether it allowed an IP address or not. This was a binary criterion: yes or no. Today, we're moving towards a situation where the mail server says: No, we won't decide so early. We will let the email through. We will look at the blocklist and check whether the address is listed or not. And we will check other parameters – for example, whether this domain has behaved properly in the past or whether it has sent junk. How can I tell that it is the right domain? Are the systems that are currently contacting me even allowed to send stuff to me on behalf of this domain? And so on.

All of these things are now lumped together and then a weighted decision is made. This so-called reputation of a system has become much more important and prominent. By the way, this is also the way we get a handle on IPv6-based mail servers. We know hardly anything about their IP address. But we know if the sender domain is OK, if the sender domain allows what this IPv6 address sends, etc. This all feeds in to the reputation.

---

***Reputation is something that spammers can't build up quickly. When you've misbehaved three times, you're just branded.***

---

The good thing is, reputation is something that spammers can't build up quickly. When you've misbehaved three times, you're just branded. But if you behave well all the time and then suddenly have an outlier, others can let it pass, because it's not your standard behavior. This is the reason why reputation-based systems will be the ones to win the race in the long run. This is also the reason why we have been dealing with the whole topic of sender authentication in the Email Competence Group this year at eco. Meaning SPF, DKIM, DMARC. It's all about sender reputation.

**Steffen: Do you usually use a list, or a provider, or do you put together a portfolio? And if so, how do you do something like that? If you look at the paper, you see different lists from one provider. How does this work?**

---

***The free lists do help, but they are nowhere near as effective as lists you pay for.***

---

**Koetter:** There is this saying: "You get what you pay for". This is actually true in the area of blocklists as well. If it is really important to you that you receive as little spam or malware as possible, then you need to sign up for a subscription so that you can query this data live. You might get the data elsewhere, but it might be 5 or 10 minutes old. And in 10 minutes, the critical cases are already through. The free lists do help, but they are nowhere near as effective as lists you pay for.

And if you want to think about it further, the two big players on the market right now are Abusix and Spamhaus, and if you take something from them, you are guaranteed not to be doing anything wrong. On the other hand, if you go for providers that don't have a delisting process, or even want to take money for delisting, then you can be sure you're doing it wrong. There are now also so-called meta lists provided by specialized service providers. These focus on different aspects of abuse and filter, for example, only email systems that are not RFC-compliant, or include only systems whose sender domain has been abused, or include only mail systems that have sent emails that contained links to malware. The big operators take this knowledge from the smaller, specialized lists and consolidate that into one big list for themselves.

What also happens, again and again, is that people create lists based on private projects, and these are not always continuously maintained, because of the amount of work involved. As soon as the enthusiasm fades, then the list ceases to be up-to-date. It makes sense not to include such lists, because they no longer do anything but cause harm. So you should check your lists regularly. If you run a mail server privately, do what you want. If a business is going through it, it's best to pick lists where you can get a guarantee of performance. Such lists do not cost a fortune, but they do cost. We are, after all, dealing with a commercial Internet. If your business depends on these systems working, then it's worth it.



**Patrick Ben Koetter, Leader of the Email and Anti-Abuse Competence Groups, eco - Association of the Internet Industry, Member of the Board, sys4 AG**

*Patrick Koetter is an email expert, and a board member of sys4 AG, which specializes in email, DNS, and the development of highly secure platforms and services. He contributes his knowledge and experience to eco as an expert and as Leader of the Email and Anti-Abuse Competence Groups.*



**Lars Steffen, Director, eco International, eco - Association of the Internet Industry**

*Lars Steffen is Director International at eco – Association of the Internet Industry (international.eco.de), the largest Internet industry association in Europe. At eco, he coordinates all international activities of the association and takes care of the members from the domain name industry.*

Read this article online at: <https://go.eco.de/t8ehGR3>

[\*]sys4



magazine  
 Internet industry

# LET'S END COUNTER-PRODUCTIVE ANTI-DNS ABUSE REPORTING



Source: © IvelinRadkov | iStockphoto

**Natasha Pelham-Lacey from CleanDNS, on improving an imperfect system to lower the bar for reporting abuse and increasing takedowns.**

Bad guys already have it easy enough, why make things easier for them? Abuse complaints often receive “push back” due to unrealistic thresholds. Why?

It's not for lack of good intentions, as most industry professionals care about doing what's right. They want to end online abuse and victimization wherever and whenever they occur. Yet, while it is unfair to accuse most folks of not caring, especially those who are inundated with immense volume, the inconsistencies we find when it comes to acting on evidenced complaints cry out for improvement.

**No excuse: If it's abuse, cut it loose**

It's an all-too-common story: a conscientious company wants to do the right thing for its clients and its industry. In this case, stop abusive domains and minimize the associated malfeasance. The analysts begin with a very idealistic approach when it comes to calling out bad actors.

---

***There is a lack of consistency in dealing with abusive domains, plagued by nuance across the board.***

---

Before long, however, reality sets in. Cleaning up the Internet

is not easy, even in cases where the abuse is painfully obvious. That there is a lack of consistency in dealing with abusive domains, plagued by nuance across the board, is an understatement.

For example, bulk registrations engaging in spam cannot be considered a big problem one day and then ignored the next. And people who send us screenshots of their inboxes filled with spam messages as evidence are right that we should be able to do something about it. Their attitude is, if you are a well-intentioned, reasonable human being, please make it stop. And they're correct, we should be able to. Why, then, is it so difficult?

**Lower the bar, increase takedowns**

---

***If standards of proof, or of reporting, are unrealistic, we will not succeed in taking things down.***

---

First, there is such a thing as setting the bar too high and being too nitpicky when it comes to evidence of an abusive domain. If you require a person to send an impractical amount of evidence, they won't. If standards of proof, or of reporting, are unrealistic, we will not succeed in taking things down. The abuses are going to keep happening and we will all come off as if we are not even trying, and that's not the truth.

As the registrar or the registry, if you can see the evidence and the timestamps, you can address what's going on without placing an undue burden on the entity making the complaint. Consider a few other examples that shine a light on the at-times

absurd requirements often implemented for acting against abusive domain names.

---

***If you can see the evidence and the timestamps, you can address what's going on without placing an undue burden on the complainant.***

---

- Requiring full message headers when you have a screenshot of an individual's whole inbox loaded with spam;
- Giving a domain that is reported for abuse, and registered less than 30 days, a chance to fix the issue (it's not going to – it's malicious!);
- Only acting on some but not all bulk registrations; more specifically, reviewing individual abusive bulk registrations and not the whole group;
- Using "is it currently listed as abusive?" as a decision-making tool to determine whether you should act on a particular domain. Simply not being listed does not mean the abuse was remediated;
- Playing favorites with DNS abuse reporting sources, such as not accepting reports from one, but accepting them from another;
- Shifting an issue to another party when the first party has the authority or policy to act;
- Arguing that a website that is clearly a phish is an issue of trademark or content;
- Taking too long to remediate abuse. At what point should a decision be made to protect Internet users versus harming the site/domain/registrant?

We can all agree that the system is imperfect. Making it better begins with pointing out where there is obvious room for improvement. Furthermore, reporters of abuse should know that once they've reported it, it's in the queue. If the reporter could be confident that action will be taken as warranted, once they have reported it, they would (hopefully) stop repeatedly reporting it.

**A reasonable approach to a better Internet begins with 'us'**

---

***Standardization using a reasonable person's judgment would be enormously helpful and save lots of time.***

---

Each situation above, and there are many more, demonstrates an opportunity where standardization using a reasonable person's judgment would be enormously helpful and save lots of time. Until we do something about that, we are giving the wrongdoers an advantage they don't deserve or need.



**Natasha Pelham-Lacey, Security Analyst, CleanDNS**

Frankly, most of these points are so commonly known and discussed as to be clichés. Everyone agrees that these issues can be readily resolved. The involved parties want them resolved. Most of us share the goal of making the Internet a better place: Why make that goal so difficult to achieve? The bad actors have it easy enough, they don't need our help.

CleanDNS is about cleaning up the Internet for good. We believe standardizing how to act against abuse, using a reasonable person's judgment and following the rules, is the best way to achieve that goal. Correcting the challenges discussed above represents the first logical steps toward reducing the abuse and mitigating the victimization, all with the added benefit of saving lots of effort and creating a safer Internet along the way.

*Natasha Pelham-Lacey is a cybersecurity professional. She works with registries and registrars to help manage and mitigate their abuse. Natasha earned a Bachelor of Arts in Forensic Psychology, and a Cybersecurity Professional certificate from NJIT.*

Read this article online at: <https://go.eco.de/yOzEqU1>

**CleanDNS**



# EVIDENCE EQUALS BETTER DNS ABUSE MITIGATION



**Gia Isabella from CleanDNS addresses the creation of standards for evidence of Internet abuse to expedite the handling of abusive content.**

## **Better standards = Better results**

Consider the many advantages to mitigating Internet abuse: interdicting bad actors, reducing victimization to end-users, meeting regulatory and compliance requirements, limiting liability and growing profit margins.

Why then is DNS abuse so hard to stop? There are many reasons, and just as many potential solutions. One thing is sure, a standardized, evidence-based DNS abuse reporting process could streamline and accelerate the mitigation and takedown process.

By standardization we mean: "Here's the evidence. Does it match? Yes or no?" Under this scenario there are no judgment calls, and fewer grey areas. The bad actors get taken down posthaste, protecting users from cybercriminals and stakeholders from growing exposure to liability claims.

## **DNS abuse is out of control. Here's how we tame abuse.**

Internet abuse is persistent. Bad actors that maliciously register and compromise domain names are a constant problem for both the consumers on the Internet as well as the companies that run the infrastructure of the Internet.

---

***Today, virtually every reporter of domain abuse follows a different standard for reporting abuse to registries, registrars, ISPs and hosting companies.***

---

Today, virtually every reporter of domain abuse follows a different standard for reporting abuse to registries, registrars, ISPs and hosting companies. Evidentiary thresholds are so diverse that registrars and registries have different standards on the information needed to remediate an abusive domain. Each takes their own approach to the key question: "What evidence is needed to convince the appropriate infrastructure entity to act upon an instance of Internet abuse?" The lack of standardization for reporting is an ongoing issue for those on the receiving end of the report. That's why evidencing issues are so important.

The DNS abuse Framework exhibits the types of abuse that should be acted upon, but does not go as far as to detail how to appropriately evidence and report abuse. There are few resources beyond the Terms of Service of various providers that offer information one should include when reporting an abusive domain.

---

***The standardization of evidence would be advantageous not only to ensure quick validation of the claims, but to reduce the timeframe and shorten the victimization period.***

---

For example, currently a party reporting abuse might say, "I want you to take this abusive domain down because they're phishing me." The party reporting the abuse did not provide any evidence other than the URL, and is unaware that the domain will not be acted upon unless evidence supporting the abuse is presented. The recipient of the abuse report attempts to investigate the report but is unable to validate the initial abuse claim. As there is no standard for evidence, the abuse report submitted will be disregarded due to the report having insufficient evidence. If the reporter knows this, they will then attempt to generate



or locate the evidence, but not knowing what standards are required by different infrastructure providers causes delays all around. The standardization of evidence in this scenario would be advantageous not only to ensure quick validation of the claims, but to take advantage of this reduced timeframe and shorten the victimization period.

Obviously, there needs to be a better method via standardization. The goal should be that, when an instance of abuse is reported, all the evidence will be clearly presented to validate the abuse so that it can be remediated in a timely fashion.

### Creating standards to reduce the uptime of abusive domains

What is needed is a robust evidence standard by abuse type, and a majority of the domain name industry are working towards one. Once this standard has been developed and adopted, complaints can be quickly remediated, and victimization will be reduced.

Currently, no governing body has a standard of evidencing for domain abuse that can be deployed within all jurisdictions. Regardless of regional governmental laws, the ability to clearly assign the components of an abuse type so that it can be well-evidenced is clear. Even without a governing body there are industry groups that are pushing forward on evidentiary standards.

---

**To be effective, evidence included in reports must cover the events and substantiate the claims.**

---

But what is very interesting, whether we are talking about mobile coverage, 5G, or other forms of connectivity, is that we simply have the problem that the capacity of the construction companies doing the rollouts seems to be really stretched at the moment, because there is a huge demand for construction companies from very different industries, including IT / telco. Besides, to be effective, evidence included in reports must cover the events and substantiate the claims. Reports must be time-stamped appropriately to demonstrate when things happened, include the search bar displaying the domain or URL in question, and, in some cases, include the location and resolution of the screen when the abuse is first observed. There should be visible evidence that can be validated or verified.

---

**When a fully evidenced report is presented, the abuse can be acted upon as soon as possible.**

---



Gia Isabella, Abuse Program Manager, CleanDNS

When a fully evidenced report is presented, the abuse can be acted upon as soon as possible. By providing a report that checks all the boxes, the window for victimization shrinks dramatically. Which, in the end, is the objective behind standardization. Reduce the window of time abuse is allowed to exist, and you can reduce victimization.

### Flexibility and vigilance are key to successful abuse monitoring

Once a standard is created, another key issue is how to adjust it for maximum effect as time marches on. As criminals and fraudsters come up with new types of abuse, an evidencing pattern for that type of abuse needs to be structured and deployed immediately – improving the responsiveness to new types of abuse dramatically.

Ideally, this can facilitate the cleaning up of the Internet for good. This will bring a measure of consistency across the board and an element of clarity for everyone involved. For registries, registrars, ISPs and hosting providers, it's a win-win.

*Gia Isabella is an experienced technical security and intelligence professional. She works with registrars and registries to curate abuse programs that fit organizations' anti-abuse objectives. Gia earned a Master's of Professional Studies degree in Cyber Intelligence from Georgetown University, and a Bachelor's of Science degree in National Security from the University of New Haven.*

Read this article online at: <https://go.eco.de/dGbHAgE>

CleanDNS



# MITIGATING DNS ABUSE: TAKING A FIRM POSITION AND PROTECTING EMPLOYEES



**Kelly Hardy from CentralNic explains how companies benefit from fighting abuse and from protecting the employees on the front lines.**

At this moment, and for the last several moments, DNS abuse is the most commonly discussed topic in Internet governance circles across all aisles of interest.

The opinions on what constitutes abuse and how it should be handled vary depending on who you speak to. A government representative might, for instance, want to paint DNS abuse (and who is responsible for policing it) with a broader brush than a domain registrar or hosting provider would.

Determining what constitutes abuse, who should be responsible for fighting it, to what extent and whether content and speech should be monitored are complex issues that have been tackled whack-a-mole style within the infrastructure community for years. Just when we think we've reached some sort of consensus on what abuse is and the parameters of responsibility for it, the game changes – as is the nature of such things.

While high level arguments swirl, companies and groups which are responsible (or have elected to take responsibility) for mitigating it in real time do the difficult and dirty work of determining how to handle these situations as they arise and minding the safety of employees who are doing this hard work.

**Fighting abuse from the European registrar perspective**

When dealing with abuse from a corporate perspective, German registrar Key-Systems, which is part of the CentralNic Group (which holds memberships and advisory positions with several anti-abuse groups and organizations), like most players

in the domain space, take their cues from the DNS abuse Framework.

According to my colleague Volker Greimann, Legal Counsel for Key-Systems, in terms of abuse monitoring, third party abuse reports and a daily check of their registration database against multiple publicly available lists that report and provide evidence of abusive behavior, as well as taking direct reports of abusive behavior from third-party reporters via an abuse email address, are the foundation of their abuse program.

---

***"As a domain name registrar, our ability to take down specific content is limited, and we only have the ability to suspend or delete the entire domain name."***

---

Greimann continues: "As a domain name registrar, our ability to take down specific content is limited, and we only have the ability to suspend or delete the entire domain name. This means that the primary parties responsible for the removal of single instances of such content (e.g., where not the entire domain is used for these purposes) is the registrant and their hosting service provider. We therefore work closely with our resellers to address the specific issues we become aware of.

"Our standard processes usually involve reviewing the merits of the complaint as well as the evidence included with it and, unless the violation is immediately obvious DNS abuse, we would refer the matter to the reseller so they can address the issue with their customer(s). Where these parties refuse to act and the dangers of allowing the continued presence of such content outweigh the dangers of removing the rest of the content available under the resource, we will take such action as necessary to stop the abuse as an ultima ratio measure.

"However, as a registrar, we cannot enforce the laws of every country in the world. Therefore, we can only make determinations where the legality is in question under the jurisdiction(s) applicable to us and where the violation is obvious. This is also a reason to involve our resellers as they may be directly affected by laws that may not be applicable to us, but are to them, and are therefore able to take action under those laws."

**Abuse work is done by humans, keeping them safe is a priority**

---

***In addition to acting on abuse violation in a flexible landscape, companies doing this work also have an obligation to protect the safety of the humans taking action.***

---

In addition to the difficult job of acting on abuse violation in a flexible landscape, companies which are doing this work also have an obligation to protect the safety of the humans taking action. Although rarely spoken about in conversations regarding fighting DNS abuse, the effects of abuse are occasionally also felt by the acting teams. While abuse is fought at the corporate/business level, these decisions and policies are made by human beings who occasionally become the target of whatever group or person is perpetuating abuse. Whether it is a hate group making credible threats or accusations that lead to public irritation, the path of online recourse can include doxing, swatting, cyberstalking/bullying, threats and hacking.

Having experience with high-risk abuse situations, I have found that when acting in regard to content abuse, there are two simultaneous priorities: keeping the public safe and keeping your team safe.

---

**When acting in regard to content abuse, there are two simultaneous priorities: keeping the public safe and keeping your team safe.**

---

When looking for resources to create a protocol for employees dealing with high-risk abuse instances to follow, I reached out to Kellie Peterson from Automatic who has experience with taking steps to mitigate the above listed recourse events in the LGBTQ+ community. She provided the foundation for a prevention program that I have shared with multiple clients and companies across the tech space.

Should the need arise, the following actions are the minimum both key employees and companies should consider when acting on abuse from high-profile/high-risk groups.

#### Personal

- Enable 2 factor authentication on email accounts, gaming accounts, all social media, and banking.
- Use Google authenticator where possible rather than SMS.
- Change all existing passwords and use a password generator to create complicated non-personal passwords.
- Order a security key for your company and personal Gmail or other free service-based email account. Yubikey is great for this.
- VPN on all devices.
- Call banks, utilities and credit card companies and let them know you are a target.
- Depending on the region in which you are located, call your phone provider and ask to have a port freeze put on your account – this will prevent anyone who isn't you from intercepting any 2FA requests that come to you via SMS.
- Ask Google to remove your personal information. You can submit a request for this service by visiting the google



Kelly Hardy, Head of Registry Policy, CentralNic

help page or <http://support.google.com/websearch/answer/9673730>

#### Group

- If receiving messages, create an incident log where the date, time, description of message and result/recommendation is recorded. This should not be on an open platform such as google docs but should be kept somewhere encrypted like Etherpad.
- Install Signal, Telegram or other secure platform on your phone and desktop for secure messaging.
- For secure group conversations use Wire.
- Kill all Orphan accounts – any services or social media currently unused that might have an old password.
- Make sure security is up to date in the event of DDoS attacks.

While the full picture of what is described above, both in terms of monitoring/taking action on abuse as well as keeping your radar up for blowback that could include high stakes personal vigilance, can seem onerous at first glance, it is widely believed within the infrastructure community that all companies benefit from fighting abuse, full stop. The more consistent we are across the industry both in terms of how we handle such situations from a policy and enforcement perspective, the easier it becomes to deal with over time.

*Kelly Hardy is Head of Registry Policy at CentralNic Group PLC. Kelly helps both ccTLD and gTLD registry partners with policy issues including launch processes, rights protection, eligibility, dispute resolution and more. The former domain consultant is specialized in International Business Development, Channel Management, Policy and Marketing/PR strategy and is an expert in ICANN policy and New gTLDs.*

Read this article online at: <https://go.eco.de/yBQLIa6>



# CONTROL YOUR DIGITAL BRAND: ON THE INTERPLAY OF DEFENSIVE DOMAIN REGISTRATIONS, ACTIVE MONITORING, AND BRAND ENFORCEMENT



Source: © Who\_I\_am | iStockphoto

**Verena Kuthe from LEMARIT outlines the path to retain full control of digital brands through the best brand protection approach.**

Do you know what digital activities are circulating in the name of your company, your products, or your brand? Can you rule out the possibility of fraudulent copycats sending phishing emails in your name or product pirates using your brand to trade in counterfeit goods? Without doubt, the ever-changing digital space is an ideal venue for brands to market themselves. But along with the advantages come risks, and cybercriminals have realized that the value and power of major brands is good for their illegal business. Consequently, their gains come at the expense of legitimate brands.

Whether it is cybersquatting, domain grabbing, or unauthorized and abusive use: domains are quite often the starting point for a wide variety of cybercriminal attack vectors. Fortunately, the possible countermeasures are barely less extensive, from proactive domain management to monitoring potential trademark infringements. As the de facto guardians of the brand, trademark owners may have the greatest stake of anyone when it comes to finding the best possible interplay between those measures and gaining full control over their digital brand.

The following will outline the interplay of each approach and will take a fictitious brand and one of its products into account.

## **Optimized domain portfolio and defensive registrations**

---

***An individually optimized domain portfolio is still fundamental for controlling your brand in a dynamic and supposedly unmanageable digital world.***

---

The good news first: An increasing number of attack vectors also means an increasing number of possible countermeasures for rights holders, and in 2022 an individually optimized domain portfolio is still fundamental for controlling your brand in a dynamic and supposedly unmanageable digital world.

As part of the domain portfolio, defensive domain registrations are preemptively registered domain names with the purpose of keeping them out of the hands of competitors, scammers, and the like. Taking the size of the optimal domain portfolio into consideration, there are various motivations behind possible defensive registrations. Besides competition and among others, these can include registering typos and misspellings to avoid





**Verena Kuthe, Head of Sales & Business Development, LEMARIT GmbH**

phishing and loss of traffic. In the case of the fictitious domain brandproduct.com, this could include branclproduct.com and brandprodduct.com. It is worth having an eye on enforceability too, as different TLDs vary in how easy they are to enforce once a trademark infringement is identified.

With more than 1,500 different top-level domains, domain registrations – even for different brands, if necessary – can quickly become a bottomless pit. LEMARIT advises brands on their optimal domain portfolio to ensure they have a single, global view of their domains, enable them to ensure timely renewals, and to respond to threats and opportunities.

### **Consider the relevance of domain blocking services**

As part of the above, what are known as blocking services can also provide a means for brand owners to protect individual brands from third party registration. The advantages of another protective wall in the form of domain blocking may be obvious in view of the supposedly simple handling, but it is worth looking at the details.

---

***Domain blocking services can be an effective means in the fight against trademark infringement, but their relevance must be thoroughly weighed up.***

---

While blocked domains are protected against new registrations, they are not the same as domains that have been registered specifically and which brand owners can dispose of at any time. Domains that have been registered by third parties before the implementation also fall through the cracks with these services.

Nevertheless, domain blocking services can be an effective means in the fight against trademark infringement, but their relevance must be thoroughly weighed up.

### **Stay on track and mitigate risk by monitoring your brand**

Having the domain portfolio under control is a key step which should be complemented by several follow-up measures as part of the brand protection strategy.

For early detection of potential threats, one of these follow-up measures is the monitoring of domains, identifying registrations by third parties and thus proactively fighting cybercrime activities against your brand. Domain monitoring offers the ideal complement for domains outside the optimal domain portfolio.

As an example of the use of domain monitoring, LEMARIT would keep a close watch on online activities related to the (in this case fictitious) brand or product name, identify trademark infringements, advise the owner on possible countermeasures, and support in their implementation to get their rights back.

---

***Increased cybersecurity awareness has become essential in the protection of digital brands and IT infrastructure.***

---

With the help of Brand Protection Analysts, it is important to distinguish between irrelevant monitoring results and those that represent a real danger. Once a relevant domain has been identified, the possible next steps are manifold. In the case of brandproduct.com, the first step is to determine whether the domain is being actively used or maybe being offered for sale. Depending on the status, possible procedures can be derived. In case of non-active use, it is usually the minimum to further monitor any change made to the domain.

From an IT-security point of view, the resulting domain information gathered in the domain monitoring should be considered as threat information in the sense of cyber threat intelligence, because an increased cybersecurity awareness has become essential in the protection of digital brands and IT infrastructure. This way, partners and customers can be warned about potentially fraudulent domains at an early stage. However, the holistic cybersecurity aspect goes beyond domain monitoring and may be explored in depth on its own.

### **Brand enforcement: Fight abusive behavior**

Identifying the most appropriate actions is one of the core issues when a trademark infringement is identified. In the case of abusive use (such as fake shops, unusually high selling price, etc.), dispute proceedings are usually initiated to prohibit the use of the domain. These can vary greatly depending on the top-level domain and require an individual assessment.

However, it is worth noting that out-of-court enforcement mechanisms may get the deal done too.



As for the example of brandproduct.com, the domain is offered for sale by a third party via an aftermarket platform for domain buyers and sellers. Such an offer usually offers the opportunity to recover the domain with a monetary stake below the costs of a procedure. If the approach fails, however, the initiation of a UDRP (Uniform Domain Name Dispute Resolution Policy) procedure is still possible.

Processes like UDRP are established for the resolution of disputes regarding the registration of domain names. UDRP applies to all generic top-level domains, such as .com, while other cases may require a country-specific approach.

As a partner for all cases, LEMARIT helps to correctly assess the respective scenarios and to make a recommendation in the interest of the trademark owner – based on years of experience, expertise, and on the co-operation with specialized legal counsels in an international network.

### Control what's yours – step by step

Without any strategic approach, brand owners have little to no control over brand-related activities in the digital world. Brand protection works best when strategic prevention, detection, and response mechanisms complement one another. If brand owners choose their strategies accordingly and work collaboratively with subject matter experts to implement holistic protection strategies, they are on the right road to succeed in protecting hard-earned equity and revenues.

By the way: Wondering what happened to brandproduct.com? The supposedly cheaper purchase via an aftermarket platform fell through, so that a UDRP procedure for recovery was initiated and successfully concluded. Finally, the domain is where it belongs: In the hands of the legitimate brand.

*Verena Kuthe is Head of Sales & Business Development at LEMARIT, an 2002 founded ICANN-accredited registrar and specialist in digital brand protection. LEMARIT is based in northern Germany. Verena has been involved in the strategic development of digital brand protection for internationally operating companies for over 12 years. With the highest level of personal support and advice tailored to customer needs, LEMARIT ensures the optimal control of brands in an ever-evolving digital world.*

Read this article online at: <https://go.eco.de/R5ESimy>



# ABUSE MANAGEMENT FOR DOMAIN NAMES



Katrin Ohlmer, Managing Director, DOTZON

**Katrin Ohlmer from DOTZON looks at how domain owners can monitor and prevent abuse of their domain name to protect themselves and their customers.**

**dotmagazine: In what ways are domain names vulnerable to abuse and security threats?**

**Katrin Ohlmer:** Domains are based on the DNS, which is open "by design" and can be abused.

Often, we observe that Internet users are quite careless with domain names and, for example, click on links with fake domains. That's risky though, because scammers will sometimes use fake versions of real businesses' domains to trick Internet users into revealing personal information. We are thus of the opinion that knowledge about how to detect real and fake email addresses and domain names is a necessary part of digital education and should become common sense.

**dot: What impact does abuse have on the owner of the domain?**

**Ohlmer:** Often, the owner does not even know that his or her domain is being used for abuse. That alone is bad enough, but in the worst case, the owner can also lose access to the domain: If the registrar puts the domain on server-hold, the owner cannot use or update the owner data any more.

In cases of immediate threats such as child porn, the domain can even be taken off the Internet.

---

**Usually, a domain owner whose domain is registered under one of the new top-level domains will be informed right away if the domain is being used abusively.**

---

Depending on the type of top-level domain, domain abuse is monitored on very different scales. All operators of the new top-level domains, which started being introduced in 2014, are required by ICANN to strictly monitor any abuse. Most operators

take this obligation seriously and monitor the registered domain names under their top-level domain very closely indeed; only a few are late to the table. So usually, a domain owner whose domain is registered under one of the new top-level domains will be informed right away if the domain is being used abusively.

For operators of the country-code top-level domains (such as .de, .at or .ch) and generic top-level domains (such as .com, .info or .museum), there are no such obligations. The registry operators of these top-level domains have individual practices on how to handle abuse monitoring and management.

**dot: How do you see domain abuse developing in the future?**

**Ohlmer:** We expect two developments:

Since the GDPR became effective in May 2018, personal data are not published in the public WHOIS database anymore and it has become pretty complicated to find out about the owner of a domain based on the WHOIS.

---

***Abuse monitoring of top-level domains has become state-of-the-art and resulted in a closer monitoring of bad actors than in previous years.***

---

If criminals register a domain name for their abusive activities, the WHOIS is not the source anymore to determine the contact data – criminals can hide behind the closed WHOIS. This might lead to an increased number of fraudulent activities based on domain names.

On the other hand, abuse monitoring of top-level domains has become state-of-the-art and resulted in a closer monitoring of bad actors than in previous years.

As more and more people get online, we expect that values will be defined as to how we as global citizens want to use the Internet.

**dot: What should domain owners do to protect their domains?**

**Ohlmer:** For everyone who wishes to register a domain name, we recommend that you make sure that the registry operator of the top-level domain monitors and manages abuse. If this is the case, you should also make sure that the registry operator regularly monitors all registered domains to prevent malicious actors from misusing domain names. If not, there are many other top-level domain operators available which take this issue seriously.



Source: ©yucelyilmaz | iStockphoto

Also, there are providers like DOTZON which offer the management and monitoring of domain names for bigger domain portfolios. Many operators of the new top-level domains make use of this solution if they haven't developed the monitoring of abuse themselves. Thus, domain owners do not have to worry about potential abuse cases of their domains.

**dot: How does the DOTZON Abuse solution work, and what impact does it have for businesses?**

---

***Businesses can rest assured that the system monitors abuse and ensures that their domain names are not abused.***

---

**Ohlmer:** The DOTZON Abuse solution permanently analyzes all registered domain names under a top-level domain. The system uses data from diverse sources and analyzes abuse threats such as phishing, pharming, malware, spam, and botnets. Results of this analysis are archived according to European Data Protection Guidelines – the system is located in Germany. The DOTZON Abuse solution provides a monthly report with the results of the analysis and monitoring compliant with ICANN requirements. The DOTZON Abuse solution also provides individual reports in case of detected abuse. These reports contain all necessary information and data to act on the individual abuse case. Based on several years of experience in solving abuse cases, DOTZON has developed an abuse management process. The team at DOTZON manages abuse cases with the respective parties. The process and results of the management of individual abuse cases are documented in a report and provided to the registry.

Businesses can rest assured that the system monitors abuse and ensures that their domain names are not abused. In the rare case of abuse, the team takes care of this, and thus ensures the unspoiled reputation of domain names and the top-level domain.

*Katrin Ohlmer is an expert in Internet governance, Internet infrastructure and digital brands. She is the founder and managing director of DOTZON, a consultancy specializing in developing digital brands and identities. She regularly speaks at international conferences and supports the Internet Governance Organization ICANN in developing policies which deal with the enhancement of the namespace on the Internet.*

Read this article online at: <https://go.eco.de/oGWHEYA>



# VIGILANCE OF SOCIETY AGAINST ILLEGAL CONTENT



Alexandra Koch-Skiba, Head of the eco Complaints Office, eco - Association of the Internet Industry

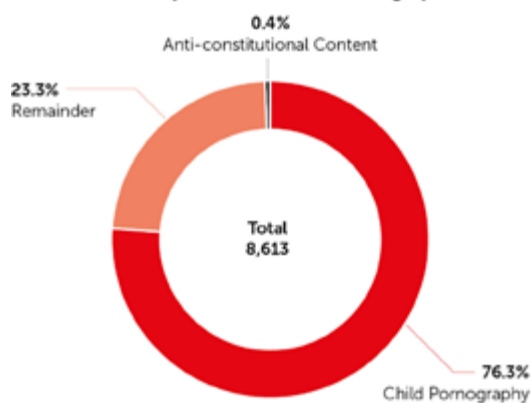
**Alexandra Koch-Skiba from the eco Complaints Office on the attentive reporting and take-down of illegal content on the Internet.**

For the eco Complaints Office, 2021 was a milestone year, marking 25 years dedicated to combatting illegal content on the Internet. We accompanied this landmark year with a campaign under the motto of "Together for the Good of the Internet."

Together with our supporters Google, Facebook, Microsoft, and other network partners, we publicly spread the message that each and every individual can make their own contribution to responsible Internet use. We also highlighted the future challenges in the fight against illegal Internet content.

In April of this year, we presented our 2021 eco Complaints Office annual report. With 8,613 actionable cases, we recorded a new high of notified legal violations on the Internet. This constitutes a rise of approximately 50 percent compared to the previous year.

Actionable Complaints 2021 (Excluding Spam)



Source: eco Complaints Office, 2022

## Depictions of abuse of children making up the majority of actionable complaints

In 2021, depictions of sexual violence against children and young people continued to account for the largest share of these complaints (6,851 cases). Accordingly, the number of actionable reports on depictions of sexual abuse and sexual exploitation of minors also increased by about 47 percent in 2021.

As sad and distressing as these increases are, especially concerning depictions of abuse of young people, they also show that our society is becoming more and more vigilant and is clearly acting against illegal content. The core message of our Complaints Office has resonated with people: Everyone can report illegal Internet content and thus actively contribute to its take-down as well as its prosecution.

## Depictions of abuse taken down in 98 percent of cases worldwide

In close cooperation with our network partners, in 2021 our Complaints Office was able to achieve important successes: Within Germany, 100 percent of hosted websites with depictions of sexual abuse were taken down within an average of 2.65 days. Worldwide, such content was removed in less than a week and with a success rate of approximately 98 percent.

---

***The core message of our Complaints Office has resonated with people: Everyone can report illegal Internet content and thus actively contribute to its take-down as well as its prosecution.***

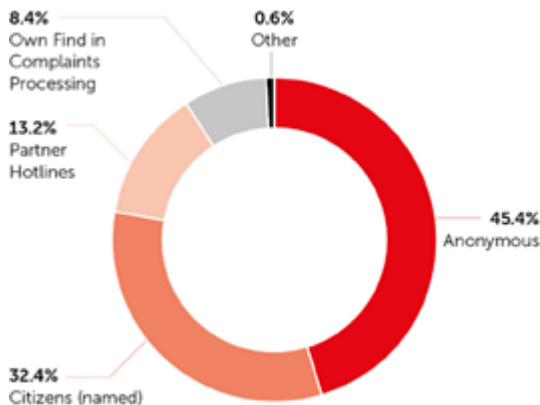
---

Depictions of abuse and other illegal content were taken down quickly and efficiently in 2021 – and this functioned on a worldwide basis, despite some considerable challenges brought about by different legal situations in individual countries. This shows that self-regulation also works internationally. In this respect, it is worth noting that only one fifth of the reported URLs were hosted in Germany.

## How citizens can report illegal Internet content

Last year, our Complaints Office received a total of 25,775 complaints about Internet content which was potentially illegal or relevant to the protection of minors. A good third of the citizens provided contact details. Approximately 45 percent submitted the complaints anonymously, representing an increase of about 20 percentage points.

Reporters of the Received Complaints (2021)



Source: eco Complaints Office, 2022

**Children and young people can grow up safely online if the Internet industry and self-regulatory authorities, policy-makers, and supervisory and law enforcement agencies work together in close cooperation.**

As in previous years, in 2021, our exchange with multiple political actors generated an enormous resonance regarding our success in the fight against depictions of sexual abuse of children, as well as anti-constitutional and other prohibited content. Our continued journey along this exchange path in 2022 is essential. Children and young people can grow up safely and age-appropriately online if the Internet industry – alongside self-regulatory authorities, policy-makers, and supervisory and law enforcement agencies – work together in close cooperation. This is also the case regarding the amendment of the Protection of Minors in the Media, which, for us as a hotline, will most definitely continue to be on our radar this year.



**harmful content**

Source: © bartamarabara | iStockphoto

**Society increasingly sensitized to harmful and illegal material**

**Our society is increasingly sensitized to the fact that material harmful to children and young people or other illegal content must not be tolerated.**

Many reports on hate and incitement on the Internet are ultimately subject to freedom of expression and are not further reported to law enforcement agencies or providers by the eco Complaints Office. As a society, we should continue to stand united for the sake of peaceful coexistence and responsible Internet use to ensure that hatred and distrust have no place on the Internet. In 2022, our anniversary motto is more relevant than ever: Together for the Good of the Internet. I look forward to further cooperation, exchange, and joint activities!

- You can download the eco Complaints Office Annual Report 2021 here:



- Illegal Internet content can be reported to the eco Complaints Office here:



Alexandra Koch-Skiba has been registered as an attorney since 2005. During her legal education she specialized in criminal law and the law of the protection of minors. As the Head of eco's Complaints Office, she is in charge of the hotline's management and of supporting the report handling, in particular in regard to legal issues. She represents the hotline at the European and national level, e.g. at European Networks, in liaising with law enforcement and other relevant stakeholders, and at events. Moreover, she represents eco on topics related to youth protection on the Internet.

Read this article online at: <https://go.eco.de/XUfu542>

**eco**   
COMPLAINTS OFFICE





# FIGHTING THE GOOD FIGHT: PREVENTING THE SPREAD OF CSAM WITH SOFTWARE



Els de Jong, Marketing Coordinator, BIT

## Els de Jong and Wido Potters from BIT, on software-based tools for combatting illegal and harmful content.

Every hosting company has issues with resource and network abuse. Abuse can take many forms, ranging from DDoS attacks to the hosting of illegal materials on servers. AbuseIO was released in December 2014 as open-source software to aid in the prevention of Internet abuse. It began as SpamCheck at BIT, an Internet technology company. When others expressed interest in the software, the decision was made to turn it into an open-source project. The software (partly) automates the handling of abuse reports, making the entire process much faster. The software is open-source and free to use for anyone who wants to. It also continues to be developed.

*"This tool has enormously increased the amount of work we can handle, by automating processes while taking into account security checks. SCARt helped us quadruple the number of URLs we can process. The result really signifies the importance of implementing smart IT when combating CSAM."* – Dutch CSAM Hotline

---

**By (partially) automating this process, analysts who would normally have to manually verify each instance of CSAM are relieved of a significant amount of mental strain.**

---

In the years following its release, the EOKM (Dutch Expertise Center for Online Child Abuse) expressed interest in anti-abuse software and asked if it was possible to develop a tool to help automate the process of CSAM (Child Sexual Abuse Material) reporting. SCARt was developed as a response to this request. SCARt is a piece of software that assists in the processing of CSAM reports and sends NTDs (Notice to Takedown) to site



Wido Potters, Board Member, AbuseIO Foundation; Manager Support & Sales, BIT

owners and/or hosters when CSAM is discovered on their sites and/or servers. SCARt also verifies whether or not illegal content was removed after the NTDs are sent. By (partially) automating this process, analysts who would normally have to manually verify each instance of CSAM are relieved of a significant amount of mental strain. In 2022, The Danish CSAM hotline (Red Barnet) also began testing SCARt.

SCARt is free to use for any organization that wants or requires it to aid the fight against the spread of CSAM on the Internet. It is not, however, freely available for download, because someone with malicious intent could modify the source code and maliciously use it for CSAM detection. Credentials must be checked to ensure that SCARt is only used by legitimate organizations and foundations. This is done by checking with other hotlines (such as EOKM) and determining whether or not the organization/foundation is a member of INHOPE (International Association of Internet Hotlines). As a result, the tool is open-source, but the anti-CSAM specific code is not available to the general public.

## How does SCARt help?

---

**By automating the system, more reports can be processed, which means that more CSAM can, will, and should be taken offline.**

---

Every year, CSAM hotlines all over the world receive a large amount of information to process because, unfortunately, there will always be illegal content on the Internet. In 2021, for example, EOKM processed more than 800,000 URLs. By automating the system, more reports can be processed, which means that more CSAM can, will, and should be taken offline.



Source: © Good\_Stock | iStockphoto

SCARt can receive URLs to process from multiple sources. ICCAM, a tool developed for INHOPE to aid the prevention of the spread of CSAM, can be linked to SCARt via an API. This connection then feeds all ICCAM reports for the relevant country (in the case of EOKM, the Netherlands; for Red Barnet, Denmark). Another option is to use an online form (so, with the help of the public). A hotline's website can include a reporting form where concerned citizens can report URLs they come across that may contain CSAM. This form is then connected to SCARt, and the processing starts.

The URLs that are fed into SCARt via the different sources are scraped for images. The images are then hashed. If the hash of an image corresponds to a hash that was marked as illegal content before (either in SCARt, ICCAM or any other database), the image will immediately be classified as illegal. Images that are unidentifiable (so no hash on file) will be processed by human analysts to determine whether or not they contain illegal content. Any illegal content will be flagged and SCARt can then automatically send the NTDs to the website owner or hoster(s). SCARt will also check if the images get taken down after the NTDs are sent.

**The future (and beyond)**

SCARt is a highly modular piece of software. Image scraping can be enabled or disabled and, instead of images, it can be configured to scrape text. More extensive logging, among other things, can also be enabled. As a result, the tool is suitable for use as a general abuse reporting tool. Government agencies can use it to prevent the dissemination of terrorist content online, banks can use it to stop phishing sites, and brands can use it to combat fake web shops. The open-source community adds features and improves the tool as it is used in more diverse ways. As a result, the CSAM hotlines will benefit.

Regrettably, the work of preventing CSAM is never done, so SCARt is already constantly being improved. One of the long-term goals is to improve the AI module to automatically classify CSAM

images, making the process faster and less mentally taxing for the analysts who now still have to view this horrifying content on a daily basis. SCARt is a non-profit foundation that is supported by grants, donations, and the effort of the open-source community. Together, we can help keep children safe.

If you are interested in knowing more about SCARt and its implementation, contact Wido Potters at [wido@bit.nl](mailto:wido@bit.nl).

*Els works as Marketing Coordinator for BIT. In her job, she is involved in all things marketing and contributes to publications for BIT.*

*Wido has been working in the Internet industry for almost 20 years, since 2006 at BIT. He is an active member of the anti-abuse community. Wido is founder of the AbuseIO Foundation and co-founder of the Dutch Anti Abuse Network.*

Read this article online at: <https://go.eco.de/308WVaM>



# CONGRATULATIONS ON YOUR NEW BUSINESS – WE NEED TO TALK



Source: © weerapatkiatdumrong | iStockphoto

**Kelly Hardy from CentralNic provides cybercrime advice for end customers and clients operating businesses online during the pandemic boom.**

With the passing of the one-year anniversary of the entire world beginning to primarily do business online, many of us in the Internet Infrastructure community have had a wish granted: that businesses big and small would take their cue from big brands and set up shop online. The wish wasn't just that businesses of all sizes would get online en masse, but that they would do so by using their own secure websites as the platform. It wouldn't hurt if they had a great, niche-specific domain name, either. The pandemic is an awful way to get a wish, of any sort, but here we are. And now that we've gotten what we want, as a community, we need to do some maintenance.

As we all know too well, doing business online comes with its own set of security issues, but our customers may not really understand what that means in a practical way. Most owners of brick-and-mortar stores pretty much know and can prepare for what can go wrong. Even if you are a brand-new startup, there is a lot of anecdotal knowledge floating around about how to handle your affairs. But for a lot of businesses coming online for the first time, while dealing with all the stress that the last year could throw at them, the breadth and depth of security issues are the last thing they need to be navigating alone.

BrandShelter's Head of Marketing, Andy Churley, has written a whitepaper outlining the unique challenges that brands have faced in this year of living totally online. All of the advice he has given to large brands applies to businesses of all sizes and is

readily shareable with clients and customers. The bottom line is that, regardless of what a business owner has prepared themselves for in terms of risk in the material world, everything is completely different for their online incarnation.

---

***Cybercriminals know (...) that these smaller brands are less well-prepared and much less well-funded to counter certain types of criminality.***

---

Churley says: "One of the advantages of doing business online is that, with a little creativity and a great web-designer, the little guy (mom-and-pop store) can successfully go head-to-head with the large brands. Unfortunately, cybercriminals know this too. They also know that these smaller brands are less well-prepared and much less well-funded to counter certain types of criminality. This makes them an even more attractive target to the criminals than the big brands."



Kelly Hardy, Head of Registry Policy, CentralNic

Some of the malicious activities that a small business newly online needs to be aware of are:

- Domain hijacking
- DDoS attacks
- Traffic diversion
- Copy-cat sites
- Fake offers of sale on social media
- Phishing attacks via email
- Fraudulent apps on mobile app stores.
- Payment fraud
- Fake reviews
- Hoax web stores on marketplace sites
- Counterfeit product lines

Churley continues: "Often smaller brands are not even aware that criminals are targeting them, because they have little or no visibility on online activities outside of their own website. It is only when their brand has been suffering reduced traffic and revenues month-on-month that these smaller online retailers cotton on to the fact that they have become prey to sophisticated online criminals. Even if they suspect they are being targeted, the majority do not have the experience or in-house resources to deal with the problem. Many admit to feeling lost and helpless in the face of a well-coordinated and well-funded criminal attack, which may well destroy their revenues and reputation."

**So, what makes online retailers so attractive to cybercriminals?**

---

***There is still a cognitive break between the idea of consequences in the physical world and the idea that what happens on the Internet isn't quite real.***

---

One of the challenges that online retailers face is that there is still very much a cognitive break between the idea of consequences in the physical world and the idea that what happens on the Internet isn't quite real. Churley explains that this results in online crime being seen in a way as "victimless".

He says: "Two main themes emerge when talking to the corporate/business victims of cybercrime:

**1. Loss of consumer trust**

When a shopper visits a mall, they visit retail outlets that spend millions on location, building, fixtures and fittings, as well as staff and stock. This capital outlay at the very least should reassure the shopper that they are shopping in a legitimate establishment owned and operated by a trusted brand and selling legitimate branded goods. The cost to criminals faking bricks-and-mortar establishments, and the ease with which they are identified and shut down, is part of the reason that there

have been so few cases of it happening – with a few notable exceptions. Online, however, it is a completely different matter. Online criminals can rapidly and cheaply create an online web-store that mimics a well-known brand and offers counterfeit goods or captures payment cards and other personal details. If discovered, the cost of setting up another similar site is minimal.

**2. Revenue diversion**

The amount of footfall in a bricks-and-mortar store normally equates to revenues. Fewer in-store visitors mean fewer sales and less revenue. Online, web visitors may intend to shop in a particular webstore but may get diverted to a completely different shop due to misleading adverts, confusingly similar web addresses, or fake online offers of sale on social media. There are many web visitors who end up shopping on fake websites honestly believing that they are shopping at a legitimate store, and ending up out-of-pocket and disappointed with the brand when the products they receive are substandard."

---

***Implementing low-cost domain monitoring will actually spot potential online criminal activity before it becomes a real problem.***

---

Fortunately for our users and clients, there are many ways to make themselves less attractive to criminals. Churley advises that: "For online brands and businesses, implementing low-cost domain monitoring will actually spot potential online criminal activity before it becomes a real problem. Before launching a look-alike website, or an email phishing attack, criminals need to register a domain name which is confusingly similar to the brand that is being targeted. Spotting these registrations as soon as they happen and blocking, suspending, or recovering the domain is usually enough to deter the criminals from persistent attacks. Domain monitoring typically costs a few thousand dollars a year and can save brand and business owners many times that in lost revenues."





If your clients or customers find themselves in this situation, there are many options for recourse:

### File A UDRP

File a Uniform Domain-name Dispute Resolution Policy (UDRP); a legal recourse method for contesting legitimacy and recovering a domain name. It is a highly effective mechanism, but a slow and costly one.

**Typical cost: \$\$\$**

### Do nothing

In many cases, a domain name will be registered with the intention of using it to perpetrate a crime against a brand owner. With so many potential targets available to the criminal, it is not unusual for the domain to expire before the criminal has gotten around to exploiting it. Sometimes a wait-and-see approach is the best and cheapest option. However, it is essential to continue to monitor the domain for potential activity until the domain has expired.

**Typical cost: \$**

### Snap-back

Also called a back-order, a snap-back is an automated mechanism where a domain name is monitored until it expires. As soon as it expires, the snap-back mechanism triggers and automatically registers the domain name on behalf of the brand owner.

**Typical cost: \$**

### Cease & Desist

If the brand owner believes that a domain name (and more importantly, the website that uses the domain name) is infringing on its intellectual property rights, it can issue a cease-and-desist notice to the domain owner. This is normally done by its in-house counsel, IP law firm, or via a specialist brand protection provider, such as BrandShelter. The notice will detail the ways in which the brand owner considers that its brand is being infringed illegally and outline the action that it requires the domain owner to take and the date by which it requires action to be taken. In some cases, it will also outline the intended actions should the domain owner not comply.

**Typical cost: \$\$**

### DMCA notice

The Digital Millennium Copyright Act is a special standard type of cease-and-desist notice. It tells a company, webhost, search engine, or Internet service provider that they are hosting or linking to material that infringes on a copyright. The party that receives the notice should take down the infringing material as soon as possible. If the site owner doesn't comply, the ISP can forcibly remove the content on behalf of the brand owner.

**Typical cost: \$\$**

### Dehost

Website hosting providers provide shared disk space on which a user can create and host a website. When a brand owner identifies an infringing domain name or website, contacting the hosting provider with a DMCA or other cease-and-desist notice can permit the hosting provider to suspend or close the web-hosting account, rendering the website unreachable. This measure can yield rapid results. However, it is usually short-lived, since the website owner can simply move their website to another hosting provider at minimal cost. Despite this, moving the website from place to place will cost the cybercriminal time and money, which may be sufficient to stop their activities against the brand owner.

**Typical cost: \$\$**

### Domain suspension by registrar

By engaging with the domain registrar through which the cybercriminal has registered the infringing domain, a business owner may persuade the registrar to suspend the domain name or the account that it belongs to. Suspending the domain name will stop the domain name from resolving to the website and even if the cybercriminal moves their website to a different hosting provider, the domain remains unreachable. Registrar domain suspension is best handled by an IP law firm or specialist brand protection provider such as BrandShelter as direct communications with known individuals in each registrar can improve the chance of achieving a successful suspension.

**Typical cost: \$\$\$**

### Marketplace sites

While not a domain name dispute, brand owners often find counterfeit products offered for sale on marketplace sites such as eBay or Alibaba. Most reputable marketplace sites have their own anti-abuse programs such as eBay VeRO program. These programs allow legitimate trademark owners to request delisting of fraudulent or illegal adverts. Due to the number of infringing listings that are normally discovered, it is more cost effective for a brand owner to work with a specialist brand protection provider such as BrandShelter in an ongoing program of discovery and takedown. Takedowns are usually rapid and protect consumers immediately. Counterfeiters and cybercriminals will normally continue to attempt to sell infringing products on these platforms unless it proves too costly for them, at which time, they will target a different brand.

**Typical cost: \$**

### Payment gateway account suspension

If a brand owner can prove fraud, then a payment gateway will automatically suspend a merchant account. Almost all payment gateways have well-established mechanisms in place to assess and suspend accounts that perpetrate fraud. These mechanisms are rapid and well-practiced and, like most anti-fraud mechanisms, require submission of proof by the brand owner.



Due to the number of payment providers and complexity of the process, it is normal for brand owners to use a specialist brand protection company, such as BrandShelter.

**Typical cost: \$\$\$**

### Uniform Rapid Suspension

Not to be confused with the UDRP, the URS process is a dispute policy that allows a brand owner to file a complaint and obtain a temporary domain name suspension. While the domain name ownership is not transferred, the domain is suspended until it is due to expire. Cybercriminals will give up on a domain name that they continue to own but cannot use. The typical time to conclude a URS case is around three weeks.

**Typical cost: \$\$\$\$**

### UDRP Recovery

Many top-level domains offer a formal abuse mechanism known as a Uniform Domain-name Dispute Resolution Policy (UDRP) with the domain registry to recover a domain name that has been registered fraudulently. If the UDRP case is won by the brand owner, the domain name is transferred into the brand owner's portfolio, ensuring it doesn't return to the available domain pool unless released by the brand owner. A UDRP case typically takes from 6 - 12 weeks and, throughout the case, the domain name will continue to resolve. While it is perfectly possible for in-house counsel to file a UDRP, it is more normal for a brand protection specialist, such as BrandShelter, to undertake this on behalf of the trademark owner in order to maximize the chance of a successful outcome, reduce costs, and speed up the process.

**Typical cost: \$\$\$\$\$**

### Anonymous acquisition

If it is deemed important to recover the domain name into the brand owner's portfolio, one option is anonymous acquisition. Typically, a domain registrar or brand protection specialist will engage in a dialogue with the domain owner and negotiate a price to purchase the domain, without disclosing the identity of the potential buyer. Once negotiations are complete, monies are deposited in escrow until the domain is transferred to the registrar, whereby it is transferred to the seller.

**Typical cost: \$\$\$\$\$**

---

### **Cybercriminals are specifically targeting brands that are moving their operations online.**

---

Each enforcement mechanism listed above has its merits and frailties. And a variety of factors from the size of the business, budget, and general level of patience may dictate what a business/brand owner feels is right for them. However, providing all the information that your clients and customers need to defend themselves in this rapidly changing landscape can help them to respond to these incidents if and when they happen, recover

quickly, and get back to what they do best.

Churley concludes: "It is clear that cybercrime is an increasing issue for all online business owners and their customers. The rate that businesses are moving online has increased dramatically due to the ongoing pandemic. Cybercriminals are specifically targeting brands that are moving their operations online. Most businesses are unprepared for the wide range of sophisticated online criminality that will be launched against them. Large and small business owners may find out that it costs their customers money and affects brand owners' revenues and reputation. Even when a business owner becomes aware of the threat against their brand, usually they have no idea how to tackle cybercrime, adding to the feeling of helplessness."

---

### **Gaining early visibility of threats is always the first step in protecting businesses online.**

---

"Gaining early visibility of threats is always the first step in protecting businesses online. By undertaking a one-time domain environment audit, or implementing a highly cost-effective domain monitoring service, brand owners can quickly identify and deal with threats online before they cause any financial or reputational damage. At the same time, they will provide effective protection to the business's customers as well."

*Kelly Hardy is Head of Registry Policy at CentralNic Group PLC. Kelly helps both ccTLD and gTLD registry partners with policy issues including launch processes, rights protection, eligibility, dispute resolution and more. The former domain consultant is specialized in International Business Development, Channel Management, Policy and Marketing/PR strategy and is an expert in ICANN policy and New gTLDs.*

Read this article online at: <https://go.eco.de/OR9Jpg3>



# BORDERLESS FIGHT AGAINST ILLEGAL CONTENT



Peter-Paul Urlaub, Attorney-at-Law (Legal Counsel),  
eco Complaints Office

**For over 20 years, the international INHOPE network has been successfully working to combat depictions of the abuse of minors, said Peter-Paul Urlaub from the eco Complaints Office in a 2021 dotmagazine interview.**

The Complaints Office of eco – Association of the Internet Industry has been fighting illegal content on the Internet for 25 years. The eco Complaints Office is embedded in the system of regulated self-regulation and has, in particular, the task of improving and promoting youth protection on the Internet. Its **2020 Annual Report** showed that the independent hotline is making a significant contribution to the take-down and criminal investigation of illegal content: With a total of 5,523 cases, the number of justified complaints with a clear violation of the law was higher in 2020 than ever before and increased by almost 19 percentage points compared to the previous year. At the same time, despite the unique circumstances brought about by Covid, the eco Complaints Office was able to successfully take action against prohibited content in 97.7% of cases – worldwide.

By its very nature, the Internet is a global medium. As such, a strong asset of the eco Complaints Office service is its international collaboration. At the heart of this lies its membership of the international association of Internet hotlines, INHOPE. In November 1999, eco – alongside seven other organizations and with support from the European Commission's "Action Plan on promoting safer use of the Internet" – founded INHOPE. For over 20 years, the international network has been successfully working to effectively combat depictions of the abuse of minors. As the international umbrella association of Internet hotlines which operate worldwide and accept complaints about illegal online content, INHOPE applies a particular focus on child sexual abuse material (CSAM). The network now consists of

more than 45 hotlines in over 40 countries.

Since June 2018, Peter-Paul Urlaub, eco Complaints Office Consultant, has been a member of the INHOPE board. He was re-elected in July 2020 and has now taken on the role of Treasurer. In an interview with Peter-Paul Urlaub, dotmagazine talks about the indispensable value of the international collaboration enabled by INHOPE.

**dotmagazine: The INHOPE network has now been in place for more than two decades. From your perspective, what was eco's motivation back in 1999 for co-founding the network?**

**Peter-Paul Urlaub:** First of all, as a small disclaimer, I should just mention that I have only been at eco since 2013, which means I wasn't in situ when INHOPE was initially founded. But of course, I have been filled in on the background at numerous meetings. When eco founded its hotline in 1996, they swiftly realized that fighting against illegal content is not just a German issue that we can handle from within Germany, just for us. From the outset, we always had cases that were crossing borders, meaning that we needed partners to work with. That was basically the motivation for putting INHOPE into place back in 1999.

---

***What was recognized early on is how critical it is to have a tiered approach – both local hotlines which collaborate with local law enforcement agencies and other local or regional stakeholders, and international collaboration.***

---

What was therefore recognized early on is how critical it is to have a tiered approach – both local hotlines which collaborate with local law enforcement agencies and other local or regional stakeholders, and international collaboration. Because we see that in Germany, too, if you're a local hotline, you have a better connection to your local law enforcement system. So if we receive a report, we will send that to our local law enforcement agencies, with whom we have a strong cooperative relationship and Memorandums of Understanding, and they know they can trust our records, they know what we deal with and that our reports are pre-assessed by lawyers.

And the second thing locally relates to cooperation with Internet Service Providers (ISPs). We know our partners here in Germany and can cooperate with them far easier than we would potentially be able to with others. This means that it is still essential to be working "on site". Furthermore, it's always better to have a local hotline that understands the language, the

culture, and that is likely to have a closer connection to any stakeholder in their country. Effectively, in starting out: language, communication, culture and borderless were basically the points that the eco Complaints Office saw as necessary for action. And this swiftly brought it home that it was necessary to work with others, as we had already started doing in the early days. INHOPE was therefore founded with seven others with whom we had already been closely working with. We all saw that it would be better to not just send around reports via email, but to work more closely together: this is where the structured international collaboration took hold.

**dot: And now at the eco Complaints Office, where you've marked your 25th anniversary with the motto, "Together for the Good of the Internet", what benefits do you see INHOPE's international collaboration bringing for the safer use of the Internet?**

**Urlaub:** One big benefit is the exchange of reports. INHOPE was mostly founded to exchange reports between the hotlines. Basically, to have a system where we could simply submit the report to a trusted partner. In the meantime, the network developed further and created a system called ICCAM that supports the report submission by sending it to the right hotline. This is something that, of course, in the end benefits the take-down time of illegal content.

---

***The first and foremost benefit is the fact that the take-down of illegal content is more secure, is swifter, and follows an agreed-upon process.***

---

Because if I don't have to search for something or run the risk of possibly sending it to the wrong person, it accelerates the whole process. As a result, the first and foremost benefit is the fact that the take-down of illegal content is more secure, is swifter, and follows an agreed-upon process – because, although this might vary slightly among some of the 45 member hotlines, everybody in INHOPE reports to law enforcement and then to the ISP in some way. Which means that the take-down of illegal content is kind of standardized.

The second significant benefit is naturally the exchange of knowledge. We have a lot of topics for which such knowledge exchange can and should happen, whether it's to do with technical support or technical tools that help us with our work. Therefore we can engage in an exchange on what tech the other hotlines use that we could also implement to improve our work.

Another topic, one that's closest to my heart, is staff welfare, given that, in the INHOPE network, we deal with particularly difficult content. So what we can now do is interact with other hotlines on topics such as seeing what do they do for staff

welfare, what tricks they use to stay resilient.

And of course, we exchange knowledge about trends and content. So if someone sees an increase of content at a certain forum or platform or a new "hiding" technique, we can exchange on that and then basically perform better.

**dot: Collaboration is a process that goes a step further than networking. Given that you're a board member of the INHOPE network: Could you describe how the work of the board functions?**

**Urlaub:** The INHOPE board basically sets the strategy for our international collaboration and discusses upcoming issues to be implemented by the secretariat and the executive director. What is really discussed at the board meetings is therefore the strategic work of INHOPE.

The pandemic times have led to everybody now being equipped with a camera and a proper Internet connection, which means now we have monthly calls for the board. This offers a bit more continuity and improves the productivity of our meetings. In the past, having monthly meetings was something that was not considered, given that such regular meetings couldn't take place on a face-to-face basis, for numerous reasons. Now, while we still have to manage time zones, monthly meetings appear to be far more viable.

**dot: Perhaps you could also provide us with one or two examples of day-to-day cooperation between the hotline teams?**

**Urlaub:** A regular cooperative action that we now undertake at a hotline level is a call with the analysts. Just as background information: an analyst works in a hotline and assesses the content. So now, at the end of each month we can discuss trends, issues and questions with the analysts. From my view, that has enhanced the network feeling. But it should be noted that, of course, there is still always the indispensable option to have a call with a colleague.

One particular example which displays the benefits of such a co-operative call with a colleague concerns a case from a few years ago where we received a report from British colleagues on child sex abuse material (CSAM).

---

***One particular example which displays the benefits of a co-operative call with a colleague concerns a case where we received a report from British colleagues on child sex abuse material (CSAM).***

---

Upon entering the site, we received the "content removed" message. Our initial thought was: "Oh, great, the ISP has already reacted." But then the colleagues who reported this to us wrote and asked: "Well, what's going on? It's still online." We were very surprised and went back to the site and once again, read the



Source: © Chinnapong | iStockphoto

"content removed" message. And that was quite odd because it didn't fit the picture. I called the British hotline and we went through everything that was different between the systems in our two countries. We checked every aspect step by step, starting with: "Which browser do you use?" "OK, we use the same now". In the end, it turned out that the only difference was their location. We basically went through every little detail until we found out that, apparently, the website where the content was hosted and the service was abused had applied the technology to prevent German youth from stumbling upon adult content – since freely accessible adult content is illegal in Germany, the website simply forbade everybody who had a German IP and/or a browser that used German language to see that content. But the colleagues from the UK, who used a browser with the default language English and an English IP could see the content. We therefore used some technical tools to basically spoof the whole thing or mimic it, and then we could see the content. Which meant that, finally, the content could be taken down. But we would have never found that out if we hadn't had a call with that level of cooperation.

To take another example: There is currently no hotline in Hong Kong. While I'm aware of the fact that there are plans to establish a hotline, it's of course a difficult situation there. With the current absence, reaching out directly to the ISP in Hong Kong is naturally challenging for us; there's the language barrier, and we're not always sure how things work there. However, in collaboration with our hotline colleagues in Taiwan, who speak the

language, we have been able to arrange a little bit more in Hong Kong, meaning that content has been taken down. Basically, the simple truth is: the more we talk to each other, the more we get done and can help and learn from each other.

**dot: Does the international nature of such work sometimes present challenges, particularly in light of countries' different legal situations?**

**Urlaub:** We have a good example here, since Germany is quite a strict country regarding laws relating, for example, to child sexual abuse or sexual exploitation material. In Germany, one aspect of this we call "Posing" content (with Posing defined as images of minors in an unnatural sexualized pose). As a result, in Germany, several legal articles prohibit the sexually connoted or sexual posing of minors; depending on the age of the person shown and the kind of depiction, Posing may represent purely an infringement of media law (Section 4 (1) 9, German Interstate Treaty on the Protection of Minors in the Media (JMStV)), or may be punishable as Child Pornography or Youth Pornography (Section 184b (1) 1b and Section 184c (1) 1b, German Criminal Code).

But these types of regulations are not the case in every country. Which means that some could say: "Well, it's not illegal here, and as such we basically can't do anything." But from what I see in our statistics – the latest of which you can see in our eco Complaints Office 2020 Annual Report – we actually do not have much of an issue with take-down of CSAM-related content;

even the content which falls under Posing is removed just as quickly as the other content regarding child sexuality – it's in the same vicinity and most hosters do not want such content on their service.

But you can also see the implications of different legal situations when it comes to content like incitement to hatred or incitement of people – in the US, for example, this falls under free speech. At the moment, there's a lot happening, due to what we can simply call "recent events". We saw in the past that if we sent something over to the US – especially if it was a German text hosted in the US – the response was either, "Well, we don't understand it" or "It's free speech", depending on the content. This has changed a lot, especially in the last years. Several companies have acted against hateful content or users. So, yes, of course there are issues regarding different legal situations, but to put it bluntly, we have the same issue here: content that is illegal in other countries might not be illegal here in Germany – for instance, rules from certain monarchic countries.

**dot: Aside from legal regulations, different companies can have their own terms of services. Do you think that they go beyond the legal regulations in terms of taking down content?**

**Urlaub:** I think I have to go here with the lawyer answer. It depends. In some cases, community standards are broader and sometimes cover other content that goes beyond legal regulations; as stated before, usually hosters do not want abusive content on their services. I have also definitely seen terms of services of hosters which state that anything that is illegal or fishy – in legal terms, harmful – is not allowed. Some even reserve the right to remove such content even if an actual legal claim is not given. So, they go a step further to be sure to be able to remove content if it's abusive in some way.

**Thank you very much for your interview!**

*Peter-Paul Urlaub is a registered attorney-at-law. In his most recent legal education at the University of Oldenburg, he specialized in legal aspects in IT and Internet compliance. He is responsible at eco's hotline for ISP relations, training new staff, technical compliance, and innovation. He has been on the board of INHOPE since 2018 and is currently the treasurer of INHOPE.*

Read this article online at: <https://go.eco.de/XjqKuMt>





# ADDING TRUST & SECURITY TO INTERNET INTERACTIONS WITH DNSSEC



Patrick Ben Koetter, Leader of the Email and Anti-Abuse Competence Groups, eco - Association of the Internet Industry; Member of the Board, sys4 AG

**DNSSEC does two things: It ensures you're talking to the right online resource, and it verifies that the information you receive has not been tampered with.**

Probably the most important core protocol we have on the Internet is DNS (Domain Name System), which is a service that resolves names which we humans can memorize easily (e.g. [www.dotmagazine.online](http://www.dotmagazine.online), or [www.eco.de](http://www.eco.de)) into numbers which are things that machines can deal with easily. This makes DNS a fundamentally important service for the functioning of the Internet.

To give you an example: If you want to go to your bank, and you type the domain name into your browser, then a DNS server will receive the query: What IP address is associated with that name? The DNS server will reply with the IP address, and the browser will know where to go to.

But when DNS was invented, nobody considered the possibility that somebody else might have an interest in intercepting DNS information and maybe tricking your browser into accepting a wrong IP address – the IP address of a different server which could be used to impersonate, for example, your bank. If you hand over your personal identification data to log in to this look-alike website, then the person controlling the "bad" server would be able to capture that information and use it in an attack against the real bank website.

So, in order to protect DNS replies and to protect applications posing DNS queries, DNSSEC was invented. It's a cryptographic technology that signs every reply with something a DNSSEC-capable computer, or resolver in this case, is able to validate.

## Adding trust and security to online interactions – talking to the right resource

So, what in a nutshell does DNSSEC do? It secures what you do on the Internet. It adds security where it really is needed. Everybody believes that DNS replies are to be trusted – but they're not, unless they're DNSSEC-signed.

---

***Everybody believes that DNS replies are to be trusted – but they're not, unless they're DNSSEC-signed.***

---

When you receive a DNSSEC-signed message (as long as your machine is able to verify the information) you will know that you're talking to the right resource and you will know that you've been given the right address. Or, if it's the wrong address, the resolver will suppress the information and the connection will fail.

So DNSSEC basically is something – due to its sheer logic – that everybody should want to have, because it's all about knowing who you're talking to.

## Encryption is only one side of the coin – what can happen when there's no authentication?

At the same time, we are still witnessing exploits on the Internet. We've just seen a really large exploit that would have been impossible if the targeted and abused domains had been using DNSSEC and not only DNS. In the case of this particular attack, someone was able to hack the DNS servers and reroute people to wrong servers. And the people logged in to websites that pretty much looked like the right websites, and they handed over sensitive information. What we're talking about here is espionage, and this particular attack is said to have originated in Iran. The attackers hacked many DNS servers, created SSL certificates to impersonate governmental websites, and tricked people from other governments and countries into logging in with their personal credentials at what seemed to be their own governmental websites. The website visitors handed over their authentication data, and then the spies were able to go to the real website, log in there using these credentials, read their mailboxes – the list goes on. What was at issue here was particularly sensitive information.

Of course, the same style of attack could just as easily be used to get hold of a company's banking credentials, or for gaining access to confidential company information.



Source: © Visual Generation | iStockphoto

---

***With DNSSEC, everybody would have known about the attack, nobody would have been fooled by it.***

---

Now, while this attack would still have been possible if the certification authority had used DNSSEC on their certificate licensing machines, if all access points were using DNSSEC, and if all smartphones and other end devices were verifying DNSSEC, this attack would not have gone unnoticed. Everybody would have known, nobody would have been fooled by it.

**If it's so good, why isn't everyone already doing it?**

DNSSEC adds complexity to DNS and many people who run DNS servers – unless they work with DNS every day – have simply put up a DNS server and added a bit of information, and it seems to just magically work. They don't really know why, but it just keeps on working. And when we ask them to add DNSSEC on top as a security layer, they kind of bail out, because it turns out that they don't understand it. They think it's too complex, so they try to avoid the topic.

---

***Encryption on its own is not everything – you've got to be talking to the right resource too: authentication must come first.***

---

But there are also a range of myths doing the rounds about DNSSEC. One criticism of DNSSEC is that it doesn't encrypt your information. What the critics actually want is for the query and the reply to be encrypted, so that nobody else is able to know what has been queried and what has been replied. While I

understand that requirement, it's not on the table when we talk about DNSSEC. This seems to be a fundamental misunderstanding of the function of DNSSEC. Just because it uses public key cryptography does not mean that it offers encryption. Its purpose is quite simply validation, not privacy. And incidentally, encryption on its own is not everything – you've got to be talking to the right resource too: authentication must come first.

**Why you should implement DNSSEC**

A further myth is that it is cost-intensive. It isn't. And it works. And you need it as a basis technology to gain other things. Things like trusted bank transactions. If you do your bank transactions online you should ask your bank if their webservers and if their DNS is DNSSEC-signed. You might end up being tricked into going to a different location, placing your bank account log-in information at the mercy of unscrupulous individuals. Here, it really is about money.

---

***DNSSEC is the basis for creating trust.***

---

The next thing is, if you are part of a country's critical infrastructure, then you on the one side should be serving information about your resources that can be validated, and at the same time you should be using DNSSEC when you transmit information to others, to make sure you're talking to the right parties. As I said before, DNSSEC does two things: it ensures you're talking to the right resource, and it verifies that the information you receive has not been tampered with. And this is the basis for creating trust.

## Authentication and encryption through DANE – ensuring a secure handshake

A use case that builds on top of DNSSEC is DANE. DANE is a standard that, in the first instance, identifies services that encrypt transport. The problem with transport layer security is that it's very secure once an encrypted session has been established, but the process of establishing the encrypted session is insecure. This is where the man-in-the-middle attack comes in. Somebody might trick you into going to a different, wrong resource, and starting an encrypted session with that wrong resource. And you pass over sensitive information to that resource because you believe you're doing it in the right way – because everything is encrypted. The thing is, yes, you're right: you're encrypting – but you're talking to the wrong resource.

---

***If you want to ensure properly secure online transactions or email transmission transport on the Internet, you want to use DANE, which uses DNSSEC.***

---

DANE fixes that. DANE uses DNSSEC as a resource to allow you to validate information you've been given. The process enables the exchange of information that helps you to verify you are talking to the right resource. Usually it's the fingerprint of the certificate of the resource you want to talk to. And this information is exchanged via DNSSEC. You are able to validate that you've been given information you can trust. And there's no way of spoofing that.

The second use case for DANE is that the mere existence of a DANE record tells the client that the server MUST offer encryption. This shields the communication from the risk of a "Downgrade Attack", which can occur if the client recognizes that a server is not encrypting, and automatically "downgrades" to unencrypted transport.

So if you want to ensure properly secure online transactions or email transmission transport on the Internet, you want to use DANE. In order to do that, you need to use DNSSEC, and you should also offer it for others to use when they are communicating with you or your online resources.

## The restore dilemma

---

***While nobody gets excited about doing DNSSEC, everyone really wants to talk to the right resource, nobody wants to be tricked.***

---

The problem with DNSSEC is that it has about the same level of sex appeal as a backup. Nobody wants to do backups, but everybody wants the restore function. And that's the same with DNSSEC. While nobody gets excited about doing DNSSEC, everyone really wants to talk to the right resource, nobody wants to be tricked. So in order to gain one thing, you need to do the other.

DNSSEC is standardized, and it's mature software. There are tools out there to support implementation. All it takes is that you need to tell the people who run your DNS server to run DNSSEC. It's not complicated. But it does add another layer of complexity that needs to be dealt with.

If you need information on how to do it, you can talk to us at eco, or you can also talk to your national office for IT security.

*Patrick Koetter is an email expert, and a board member of sys4 AG, which is specialized in email, DNS, and the development of highly secure platforms and services. He contributes his knowledge and experience to eco as an expert and as Leader of the Email and Anti-Abuse Competence Groups.*

Read this article online at: <https://go.eco.de/9eRBdpx>

[\*]sys4



## ABOUT ECO

eco (<https://international.eco.de>), with more than 1,000 member companies, is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in the development of the Internet in Germany, fostering new technologies, infrastructures and markets, and forming framework conditions. In the Competence Network, important specialists and decision makers of the Internet industry are represented, and current and future Internet topics are driven forward.

Numerous eco services help to make the market more transparent for providers and users. We support members with legal consultations, in particular regarding data protection. For all users, we work to increase security and improve youth protection.

As an association, one of our most important tasks is to represent the interests of our members in politics, and in national and international committees. As well as headquarters in Cologne and a branch office in Munich, eco has an office in the German capital Berlin, and is represented at all relevant political decision-making processes in Brussels.

eco is a founding member of EuroISPA, the umbrella organization for European Internet associations. eco also represents its members with a seat on the Council of the Generic Names Supporting Organization (GNSO) at ICANN, and is a driving force behind the Internet Governance Forum. In short: We are shaping the Internet.



## PUBLICATION DETAILS

### Publisher

eco – Association of the Internet Industry

### Editor in Chief

Harald A. Summa  
CEO, eco – Association of the Internet Industry

### Editorial Team

Lars Steffen, Judith Ellis, Eilín Geraghty, Cáit Kinsella, Ladan Raeisian

eco – Association of the Internet Industry e.V.  
Lichtstr. 43h  
50825 Cologne, Germany  
Phone: +49 (0)221 700048-0  
Fax: +49 (0)221 700048-111  
info@eco.de  
international.eco.de

### Publication Date

February 2023

### Print Layout

Hansen Kommunikation Collier GmbH, Cologne, Germany

### Pictures

All pictures without source indications were placed at the disposal of dotmagazine by the authors and are used with permission of the photographers and persons depicted.

powered by



# magazine

Internet industry



visit the web version

# dotmagazine

joining the dots of the Internet industry [dotmagazine.online](http://dotmagazine.online)



The articles published in this print edition are a selection from the following online issues of dotmagazine:



[dotmagazine.online/issues/protecting-users-and-systems](http://dotmagazine.online/issues/protecting-users-and-systems)



[dotmagazine.online/issues/safeguarding-users-and-data](http://dotmagazine.online/issues/safeguarding-users-and-data)



[dotmagazine.online/issues/building-bridges](http://dotmagazine.online/issues/building-bridges)



[dotmagazine.online/issues/the-security-imperative](http://dotmagazine.online/issues/the-security-imperative)



[dotmagazine.online/issues/digital-identities](http://dotmagazine.online/issues/digital-identities)



[dotmagazine.online/issues/building-trust](http://dotmagazine.online/issues/building-trust)



[dotmagazine.online/issues/trust-the-way-forward](http://dotmagazine.online/issues/trust-the-way-forward)



[dotmagazine.online/issues/security-trust-in-digital-services](http://dotmagazine.online/issues/security-trust-in-digital-services)



[dotmagazine.online/issues/the-heart-of-it](http://dotmagazine.online/issues/the-heart-of-it)

We thank the members of the topDNS Steering Committee for their support



eco – Association of  
the Internet Industry e.V.  
Lichtstr. 43h  
50825 Cologne, Germany  
Phone: +49 (0)221 700048-0  
Fax: +49 (0)221 700048-111  
[info@eco.de](mailto:info@eco.de)  
[international.eco.de](http://international.eco.de)

powered by

