CPH Guide to Abuse Reporting Practices

Introduction and purpose

General abuse reporting requirements
- Where the issue occurred
- What happened
- Who the reporter is

Type-specific abuse reporting requirements
- DNS Abuse
  - Additional complaint requirements for phishing
  - Additional complaint requirements for spam
  - Additional complaint requirements malware
- Trademark infringement
  - Trademark infringement in domain names
  - Trademark infringement in website content
  - Additional complaint requirements
- Child abuse & child sexual exploitation material
  - Additional complaint requirements

How to submit abuse reports

Introduction and purpose

This document presents guidelines for submitting an abuse report to a domain name registrar. In rare circumstances where the registrar is non-responsive, these may also be used to submit an abuse report to the domain name registry

At the outset, it is important to define **DNS Abuse: malware, botnets, phishing, pharming, and spam, (when it serves as a delivery mechanism for the other forms of DNS Abuse)[1].**

Other cases of domain name misuse are usually better-addressed by hosting providers or registrants directly as registrar actions will be limited to informing their customers of the reported abuse. These complaints most often focus on a website's content, or **Website Content Abuse**.

Most countries have laws that regulate hosting and website publishing activities, and these laws often include mandatory reporting elements as well as a standard complaint submission form

[1] https://rrsg.org/wp-content/uploads/2020/10/CPH-Definition-of-DNS-Abuse.pdf

that the hosting provider or website publisher must make available to the public. This document does not replace due process or other applicable law, and **when dealing with abuse the web hosting or publishing provider should always be engaged prior to contacting the registrar** because they have specialized tools and granular access to address the abuse occurring on their systems, as well as a direct relationship with the users of their services. [To find out who is hosting the site in question, click here.]

ICANN's Contracted Party House (CPH)— hope to provide education and guidance regarding the abuse complaint process to assist law enforcement, lawyers, and other complainants in submitting clear and well-formed complaints to the appropriate parties, resulting in a positive and proportionate response.

This is a living document, intended to create a collaborative conversation and body of work leading to more effective methods of reporting and handling abuse complaints within the internet community. It is a platform for feedback and is not a finalized set of practices; registrars and registries continue to set individual requirements and processes for handling abuse reports.

The first section of this document outlines general abuse reporting requirements, with additional requirements for specific types of abuse in subsequent sections. Finally, there are suggestions for how to contact the domain name registrar and identify other technical intermediaries, including the web hosting provider.

General abuse reporting requirements

Content abuse should be directed first at the hosting provider, registrant, or email provider, who have the closest relationship to the content and can take the most effective action. As between registrars and registries, initial reports of DNS Abuse should be made to the registrar, as it is typically best-suited to address DNS Abuse. DNS Abuse may be reported to a registry, but the registry's role is typically limited to providing notification and an opportunity to address the DNS Abuse to the registrar prior to taking any action at the registry level. Registrars are committed to investigating and addressing abuse complaints in a timely and reasonable manner. However, registrar compliance teams often receive complaints that do not contain the necessary information to allow them to take action.

The list of requirements below is for complaints across all types of abuse. Reporters **should provide as much of the requested information as possible to facilitate efficient handling by the registrar as incomplete complaints may not result in investigation**. Registrars will be more able to respond effectively to an abuse complaint when presented with thorough, relevant information.

Where the issue occurred

- Domain name(s) being complained about, 'defanged' if possible
- Specific URLs or subdomains within the domain where the abuse is occurring, if applicable
- Webhost, if known

As a best practice, especially in the instances of alleged phishing or malware, domains and URLs should be provided in a "de-fanged" form whenever present in a report meant to be processed by humans, meaning they are adjusted such that the website address is clear but the link cannot be inadvertently followed. This is to ensure that the recipient does not accidentally click through and receive the malware, view the abusive content, etc. For example, the URL example.com could be changed to example[.]com. A prefix such as "http://" is not necessary. A person reviewing the request can easily identify the domain in question while there is no risk of unintentionally following the link.

Reports using machine-readable formats such as ARF should strictly follow the respective format specifications.

Note: all abuse concerning the same domain name should be grouped into a unique report. Sending one report per URL (for example: abuse1.example[.]com and abuse2.example[.]com) concerning the same domain name will delay registrars' time of response and increase the risk of having duplicate reports blocked by registrar spam filters.

What happened

- Thoroughly outline the situation and describe the harm occurring
    - Indicate steps necessary to replicate the abuse
- Provide information about the context and severity of the abuse, including any related evidence
    - If possible, include relevant and readable screenshots and/or links to information supporting the abuse claim as well as links providing direct evidence of the abuse
- If possible, provide the date and time when the abuse occurred, including the jurisdiction where the abuse occurred
- Describe the nature of the harm (e.g. physical, monetary), in relation to a person, client, business, or group
- Describe the desired outcome from reporting the abuse
    - This could include things like suspension or nameserver change (so any related services do not work), transfer lock (so the registration service provider cannot be changed), and requests for confidentiality
- Indicate if the complaint has already been sent to the web host, including any response,if applicable

- Evidence of any previous contact with website publisher or domain name registrant regarding the complaint, including any responses, if applicable
- If known, the age, or how long the domain has been registered for

Who the reporter is

- Complete contact details for the reporter
- Status as a representative of a government or law-enforcement agency, if applicable
- Willingness to indemnify the registrar for any action taken, if applicable

If a registrar cannot determine what abuse is taking place, cannot verify or confirm the abuse, or if the activities fall outside the registrar's applicable law and/or abuse policy, the registrar will be unlikely to take action. Also, incomplete or misdirected complaints burden registrar abuse teams, resulting in slower response times to actionable complaints. **Following these guidelines helps registrars more effectively investigate and respond to abuse complaints.**

Type-specific abuse reporting requirements

DNS Abuse

Many online security threats are the result of a malicious actor accessing a legitimate domain registrant's web hosting account, affecting a single page or entire website linked to a domain name, email at that domain, or other related resources. The registrant or hosting account holder may have no knowledge of the abuse taking place using their domain name; these situations are known as "compromised" domains.

Registrars will be unable to take action on a reported abuse if they are not also the hosting provider or email service provider for the domain in question, unless the existence of abuse can be validated internally or through a trusted source. And, to reiterate the definition of DNS Abuse, action will typically only be taken on a spam message if it is used as a delivery mechanism for other forms of DNS Abuse.

Additional complaint requirements for phishing

- The domain name, brand, or business the phish is mimicking
- If possible, an example phish email, including all available email header information from the alleged complaint (including IP addresses, relays, senders, etc.: the detailed technical information). This is necessary because email-spoofing can make an email address look like it's coming from one domain while the headers show that it came from a different domain. This helps us identify the actual domain and email servers at issue.

- Screenshots of both the complaint domain and the target it imitates, including the URL portion of the browser, if possible. This can help us identify the phish if, for example, if it is location IP-based or requires special browsers or hardware (for example, mobile vs. desktop).
- Subdomains or full URLs of alleged phishing destinations on the core domain.

Additional complaint requirements for spam

- A copy of a spam email, including the full email header information, including the information described in the phishing requirements for headers.

Additional complaint requirements malware

- Evidence of the distribution of malware

Trademark infringement

Trademark infringement in domain names

If the domain name itself infringes on a registered trademark, the most effective course of action is the Uniform Domain-Name Dispute Resolution Policy ("UDRP"). When a trademark infringement complaint is sent to the registrar of record outside of the UDRP process, the registrar will, in most cases, direct the complainant to file a UDRP complaint. Some registrars may also forward the complaint to the domain owner, allowing them to address the complaint directly with the complainant. In order for any action to be taken on a domain, the registrar of record in most cases must be presented with a valid court order or have the consent of the registrant.

The Uniform Rapid Suspension ("URS") process offers a lower-cost, faster path to relief for trademark owners experiencing clear-cut cases of infringement. Both registries and registrars recommend that an aggrieved party consider use of the URS process as an alternative path for the resolution of an alleged trademark-infringing domain.

Trademark infringement in website content

Registrars are a poor venue for a website content trademark infringement complaint as they typically do not provide or control the hosted content (unless the registrar is also the hosting provider) and thus cannot target specific content on a website; instead, **the complainant should contact the web host or otherwise follow legal due process.** Registries are even further removed from the hosting of the content and are not an appropriate party to address questions of website content abuses. Domain registrars cannot adjudicate legal disputes and will most likely not take action against the domain based on a content complaint unless it passed through approved ICANN arbitration procedures (i.e., UDRP and URS) or is

accompanied by a valid court order from the registrar's jurisdiction. In addition to complying with local law requirements for reporting trademark infringement, following the recommendations above in 'General Abuse Reporting Requirements' will assist a registrar in investigating the complaint and encourage a timely response. While trademark issues found within content are generally inappropriate to resolve at a Registrar, submissions should include the following information.

Additional complaint requirements

- Evidence that the complainant is the trademark holder or an agent of the trademark holder
- Reference to the relevant law under which the trademark abuse is alleged

Child abuse & child sexual exploitation material

Registrars and registries alike take complaints of child abuse or sexual exploitation material very seriously but are not able to review allegations of child abuse imagery as accessing such content may put the registrar in violation of applicable laws. As such, **do not send examples of child abuse or child sexual exploitation material to a registrar or registry. Instead, all complaints about child abuse material must be sent to the appropriate national authority,** such as the National Center for Missing and Exploited Children (NCMEC) in the United States or the Internet Watch Foundation (IWF) in the UK. (You can find your local reporter at INHOPE; otherwise, please contact your local law enforcement to report it.) The registrar will take action on the relevant domain upon direction from the national authority.

Additional complaint requirements

- Provide the defanged URL **only** and do **not** send examples to the registrar
- All concerns about child abuse or exploitation material must be sent to the appropriate national authorities.

How to submit abuse reports

First, complainants should ensure they have correctly identified the registrar of record for the domain in question. This can be done using a Whois lookup, either on the Registrar's website, or via a generic service like lookup.icann.org.

A key to submitting a useful abuse report—one that will result in concrete actions to stop the abusive behavior—is the proper routing to the entity best suited to take action. In a large portion of the cases, the reports should be sent to the hosting provider serving the offending content or the DNS provider ultimately responsible for resolution of the domain name involved in the abuse

incident. The mitigation actions available to these types of providers can cause less collateral damage and often allow for the opportunity to engage with the user of the abused resources. Registrars might be engaged as a followup, when the previous attempts have failed. The reason for this is that, although registrars have the ability to take swift action to address the abuse incident by breaking name resolution for the involving domain name, this swiftness comes at the risk of causing collateral damage.

Most Registrars provide forms to assist with reporting abuse at their websites, which help the reporter provide all necessary information.

Nameserver information can often be used to identify a web hosting provider, so that a complaint can be submitted to them. For the relevant domain, do a Whois lookup and find the Nameserver information; then go to the domain name found in the Nameserver hostname or do a Whois lookup on that domain itself to identify the service provider. There are some cases where the Nameserver information does not identify the hosting provider (e.g. where a reverse proxy service is being used) or lead to the abusive DNS resource, but Nameservers are typically a good starting point.

Registrars will soon provide the public and reporters with a tool aiming to simplify the identification of the applicable service provider. This document will be updated with the applicable URL when available.

Be sure to provide all the information described in the sections above when submitting an abuse report to a registrar or web hosting provider.