

Reporting abuse

This article explains how to submit a complaint about a domain name to our team. As the registrar, we will notify the relevant reseller; however, we cannot make judgments about website content, nor can we transfer a domain to another owner or registrar. For such matters, please refer to our formal [Abuse and Complaints Policy](#).

As a large registrar, some domains under our management may be misused for fraudulent webshops, phishing, copyright infringements, or other forms of abuse. If you encounter such domains, please report them to our abuse department via this website: <https://abuse.registrar.eu>

Common misunderstanding while reporting abuse:

Before submitting an abuse report, please be aware of a very common misunderstanding: Domain registrars like Openprovider manage domain name registrations (for example, yourexample.com or yourownbusiness.nl). We maintain the technical link between a domain name and the services it connects to but we do not host or control the website content displayed under that domain. If you have concerns about a website's content, please contact the website owner or the hosting provider directly, as they are the ones able to review and remove the material in question.

Contacting the Domain Owner

The domain owner (registrant) can usually be reached in one of the following ways: Through the website itself: You can look for a "Contact," "About," or "Legal" page. This is usually the fastest and most direct way to reach the website owner.

By performing a Whois lookup : Check for a "Registrant Email" address or a privacy contact form. If privacy protection is active use the contact form included in the Whois results to send a message through the privacy service.

Openprovider cannot forward messages or mediate between you and the registrant regarding website content.

Finding the Website's Hosting Provider

If the issue relates to where the website is hosted, you can often identify the hosting company by checking the domain's Name Server (NS) records via a Whois lookup.

Example:

Name Server: ns1.hostexample.net

Name Server: ns2.hostexample.net

The part after "ns1." or "ns2." (in this case, hostexample.net) often points to the hosting or DNS provider. In some cases, the domain may use a security or performance network (such as a content delivery network), which does not host the website itself. If so, visit that network's website to find their abuse reporting page or guidance for identifying the underlying host.

At Openprovider, we understand it's not always easy to determine who is responsible for a website's content. However, reaching out to the correct party (the registrant or hosting provider) ensures your concern is addressed efficiently and by the people who can act on it.

Information for the complainant

If you wish to report an abuse case, please contact us by completing the [contact form](#). To help us act more efficiently, include the fraudulent domain name and a clear explanation of why you believe the domain is being misused.

As the registrar, we may take immediate action in certain cases, such as DNS abuse. In other situations, however, we are required to follow defined processes before taking further steps.

Examples of abuse that we can address immediately:

Phishing & Pharming

Examples:

- Fake websites imitating legitimate services (e.g., banks) to steal personal information.
- Deceptive emails that appear to come from trusted sources in order to capture login credentials.
- Redirections from legitimate websites to fraudulent ones.

Required Evidence:

- Full URLs of the suspected phishing sites or screenshots clearly showing the fraudulent content.
- Copies of phishing emails, including complete email headers (with IP addresses and sender details).

What Happens Next:

- If phishing is confirmed, we will take immediate action to suspend the domain.
- If the provided evidence is insufficient, we will escalate the case to the reseller or hosting provider for further investigation.

Malware & Botnets

Examples:

- Websites distributing malicious software (e.g., ransomware, spyware, trojans).
- Domains used to control botnets engaged in illegal activities.

Required Evidence:

- Malware scan results, antivirus or security logs, or screenshots showing the malicious behavior.
- URLs associated with malware distribution or botnet command-and-control.

What Happens Next:

- If confirmed that the domain is spreading malware, we will take immediate action to suspend it.
- If the evidence points to a compromised subpage or hosting account, we will refer the case to the reseller or hosting provider for remediation.

Examples of abuse that conditions need to be met for us to act:

Pharmacy & Drug Complaints

Examples of Abuse:

- Websites selling illegal or unlicensed drugs without valid prescriptions.
- Online pharmacies offering controlled substances (e.g., opioids) without proper authorization.

Required Evidence:

- Official reports from law enforcement or government agencies.
- Proof that the pharmacy is operating without a valid license.

Jurisdiction:

- Action can only be taken if the jurisdiction of the reporter aligns with both the domain holder's jurisdiction and our company's jurisdiction.
- If jurisdictions do not align, the case must be referred to the appropriate local authorities or to the reseller/hosting provider for further handling.
- Openprovider has jurisdiction on these locations - Netherlands, Spain, Russia, India, Canada.

What Happens Next:

- If all conditions are met and sufficient evidence is provided, the domain will be suspended.
- If the evidence is insufficient or falls outside our jurisdiction, we recommend contacting your local law enforcement or reaching out directly to the hosting provider, who can take the appropriate action on their servers.

Child Abuse Material (CSAM)

Examples of Abuse:

- Websites hosting, distributing, or sharing illegal content involving minors.

Required Evidence:

- Verified reports from trusted child protection organizations or law enforcement authorities.

What Happens Next:

- Upon receipt of a verified request from law enforcement or a recognized child protection authority, the domain will be suspended immediately.
- If the report does not come from a trusted authority, we will escalate the matter by notifying the appropriate agencies for further investigation.

At Openprovider, we treat all CSAM allegations with the utmost seriousness and are committed to supporting the enforcement of laws designed to protect children online. However, as a registrar, we are neither permitted nor equipped to validate such allegations ourselves, and we cannot require

employees to review suspected CSAM material.

We strongly encourage you to act swiftly and report suspected CSAM directly to law enforcement in your country. You can find the appropriate reporting channel via the [official INHOPE website](#).

Intellectual Property (Trademark)

Examples of Abuse:

- Unauthorized use of trademarks, copyrights, or patents.

Required Evidence:

- A valid court order or a complaint from a [trusted authority \(e.g., WIPO\)](#).
- Proof that the complainant is the legitimate trademark holder or an authorized representative.
- Reference to the applicable law under which the alleged infringement falls.
- Clear URLs and file paths where the infringement occurs.

Special Note for India:

- If the domain is registered under Indian jurisdiction, you may also file a complaint under India's [Intellectual Property Rights \(IPR\) policy](#).
- We will act in accordance with legal rulings issued by the relevant Indian authorities.

What Happens Next:

- If a court order or ruling is provided, we will suspend the domain.
- If the evidence is insufficient, we will advise you on pursuing official legal channels, such as the Uniform Domain-Name Dispute Resolution Policy (UDRP).

Other Illegal Activities

Examples of Abuse:

- Online activities prohibited by law, such as financial scams, illegal content distribution, cyberstalking, or the sale of contraband.

Required Evidence:

- Official requests from law enforcement authorities or valid court orders.

What Happens Next:

- As a registrar, we cannot take direct action on these cases unless they involve phishing, malware, or other forms of DNS abuse.
- We strongly recommend reporting such illegal activities directly to law enforcement or contacting the hosting provider, who can act more quickly to remove or block the content.

Examples of abuse we do not act:

Spam (Not Phishing or Malware)

Examples of Abuse:

- Mass-distributed unsolicited emails, such as irrelevant marketing or promotional offers.

Required Evidence:

- Sample spam emails, including complete email headers (with IP addresses and sender details).

What Happens Next:

- Domains will **not** be suspended solely for sending general spam, unless the activity is directly linked to phishing, malware, or another form of DNS abuse.
- For regular spam issues, we recommend managing filtering settings through your email provider or contacting the hosting provider for further assistance.

If, after contacting us, the issue remains unresolved, you may submit a formal complaint to **ICANN** (<https://www.icann.org/compliance/complaint>) or to **WIPO** (<https://www.wipo.int/portal/en/>).

Please note that only upon receiving a formal resolution from these authorities are we authorized to delete or transfer a domain.

Information for the reseller

When we receive a complaint, we immediately forward it to the reseller and mark the domain as **“abusive.”** The reseller will receive an email notification containing details of the complaint along with a response deadline.

Response Timeline:

- In most cases, the reseller has **5 days** to address the issue and provide a response via the control panel.

- The abusive domain will be highlighted in the control panel, and accessing its details page will display a pop-up with the full abuse report.
- In specific cases, a different deadline may apply (this will be stated in the email).

Response Requirements:

- The response must clearly explain how the abuse was resolved and what measures are in place to prevent recurrence.
- If the complaint is invalid, the response should provide a clear explanation of why the complaint is incorrect.

Failure to Respond:

- If no response is submitted by the deadline, the domain may be suspended and rendered inactive.
- If a domain is reported as abusive, a pop-up will appear in the control panel.
- At any time, you can respond to the report and activate the domain again.

Domain reported as abusive

This domain has been reported as being abusive. The following reason was provided:

[Redacted text]

are suspected of uploading a video on the website. It seems all right. Please review this registrant and check the content he has uploaded on the websites. Please let us know in case you have had contact with the registrant about this case.

We kindly request you to investigate this report and fix the problem. If the source of abuse has been removed, you can write down details about the solution below and activate the domain again.

Report message *

Type your message here

Send report and activate domain

Note: From [Domains Overview](#), you can filter abusive domains by selecting the option **Show only 'abusive' domains**.

Search within your domains

Type a domain name here		Choose extension	⌵	⌵	🔍
Customer	Search in comments				
Type search query here					
Status	Auto-renew				
Select status	⌵	Select autorenew type	⌵		
Nameserver group					
Select nameserver group	⌵				
☐ Show only WPP domains		☐ Show premium domains			
☐ Show only deleted domains		☒ Show only 'abusive' domains			
☐ Show only domains with premium DNS					

Depending on the nature and severity of the complaint, Openprovider may take one of the following actions:

- **Only Notify** – We forward the complaint to the reseller without scheduling follow-up action. This is typically applied to requests such as the removal of specific information from a larger website or cases where malware is distributed through a subdomain.
- **Suspend Domain** – If the reseller does not respond by the deadline, the domain will be suspended (inactivated). As a result, the website, email, and any related services will stop functioning. The reseller can lift the suspension at any time by submitting a valid response through the control panel.
- **Delete Domain** – In exceptional cases, we may be required to delete the domain name from the registry entirely. This measure is taken rarely and only when mandated by law, policy, or authoritative rulings.

Revision #5

Created 2026-08-20 12:03:15 UTC by Sarath

Updated 2026-08-31 13:57:45 UTC by Sarath