Registrar Guide to NetBeacon Reporter

This document guides you through the process of creating a NetBeacon Reporter account, and implementing the settings to use the service successfully.

- Create an Account
- Select your settings
- Reporting Abuse
- Manage your incidents
- Manage your reporters
Create an Account

1. Browse to https://app.netbeacon.org/

2. Use the Google OAuth, or the Sign Up link to create an account. Because we want to affiliate your account with your Registrar, it is strongly recommended to use an email address affiliated with your Registrar.

   You can review the NetBeacon Privacy Policy here, the Abuse Reporter Terms of Use here, and the Abuse Report Recipient Terms of Use here.

3. You will receive an email, click the link to confirm your account.
4. Claim Your Registrar
   a. Click Settings
   b. Under Identity
   c. Click Verify as a Registrar or Registry
      
      ![Image](image1.png)
      
      d. Select your Registrar from the drop down, read the Terms of Use, agree to the Terms of Use, and click Confirm
e. This will need to be verified by a NetBeacon Reporter administrator. Once this has been completed, you will see green verification badges.
Select your settings

1. Click Settings in the top right
2. Select Alerts
3. This screen has options for you to:
   a. Choose the email address to receive abuse reports
   b. Select the types of reports you want to receive
   c. Choose abuse report format and frequency
   d. Select enrichments you find helpful and turn off enrichments you don’t want
4. When finished, click save
Reporting Abuse

Anyone can report abuse. While we expect registrars to mainly receive abuse reports, you can also report abuse. Reporters should note that their email address will be sent to the recipient of the report (Registrar), for more information see the Privacy Policy: https://app.netbeacon.org/privacy

1. Click Report Abuse on the top right
2. Enter the domain name, this will populate the registrar
3. Select the type of abuse (phishing / malware / botnets / spam)
4. Note the required information
5. Click Continue

Report Online Abuse

We’ll walk you through everything you need to provide a meaningful, actionable online abuse report.

To start, please enter the address of the website or page you’re reporting.

1. Suspect site
   Share a direct link to the site or page you’re reporting.
   
   [Input field for domain name]

2. Registered with RegistrarSafe, LLC [IANA ID: 3317]

3. Type of Abuse
   - Phishing
     Phishing attempts to trick people into sharing important personal information—banking information, login, passwords, credit card numbers. Information gained in phishing attempts can be sold and used to defraud individual victims. [More info]
   - Malware
     Malware is software that is inserted to gain access to a user’s computer to steal information or turn the infected device into a drone in a larger botnet. Malware can appear as legitimate software but with changed code, users may not notice. [More info]
   - Botnets
     A botnet is the name given to a network of personal computers, or other devices that are infected with malicious software without the individual user’s knowledge. Botnets can be used to send spam and in online attacks against websites or institutions. [More info]
   - Spam
     Spam is a volumetric game and is broadly defined as messages that are sent en masse to as many people as possible. Spam is often used to send inappropriate or irrelevant marketing messages, phishing attempts, and other attempts at online abuse. [More info]

4. What we’ll need...
   - Required Information:
     Registrars need to see clear evidence of abuse before they’re able to take action. We’ll need:
     - The date you visited the web site
     - Your location at the time
     - The company or institution being impersonated
     - A brief description of the abuse event
     - Any files that can serve as additional evidence of the abuse

5. Helpful Information:
   The following will greatly help investigators but are not required.
   - The email address that sent the message directing you to this site
   - The email headers
   - The body of the message
6. Enter the required information
7. Click Submit Report

- Date of Incident
  - The date you visited the web site.
- Your Location
  - Your geographic location at the time of the incident.
- Institution Targeted
  - The name of the company being impersonated.
- Sender Email
  - Provide the email address that sent the phishing message.
- Message Headers and Body
  - Provide the email headers and the body of the message.
- What Happened?
  - Provide a brief description of the abuse event.
- Additional Evidence
  - Share any files (e.g., screenshots) that might help.

8. You will be notified that your report has been received by NetBeacon Reporter for enrichment and routing.

Report Received
We have received your completed domain abuse report. Your report ID is 752442, and the status of your report can be found here.

CLOSE

9. You can view the report by clicking the link, or by navigating to Reports
Manage your incidents

Once a report has been submitted, it is enriched with additional information (customizable in your settings) and becomes an incident.

Incidents are automatically sent to your Registrar via your selected method. You can however view incidents from the past 30 days.

1. Navigate to Incidents in the top right menu

2. Click on an individual incident. From here you can mark the incident as:
   a. Useful (thumbs up) or not useful (thumbs down). If you think there is a reporter abusing NetBeacon Reporter, you should flag their report as a thumbs down, so administrators can review their reporting.
   b. Closed. You can use this for your own records to indicate the incident has been dealt with.
Manage your reporters

You can manage your reporters to help you organize your abuse reports.

1. Navigate to Settings on the top right
2. Select Reporters
   a. Labels: Use the free text to create a label. This will go into the subject line of the email / title of the ticket. You can then use your own automatic rules. For example, you might want to indicate the type of reporter (e.g., government, industry, law enforcement, civil society), or the type of relationship you have with that reporter (e.g., reporting since 2022).
   b. Reputable toggle: You can use this binary toggle to indicate if your organization believes this reporter is reputable. This will also be attached to the reports you receive. Currently, it is not visible to the reporter, or to other users of NetBeacon Reporter.
3. Click Save when you are finished.