

# 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/>



## Log in to your account



or

Email Address

CONTINUE

Don't have an account? [Sign Up](#)

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.

Notice

Check your inbox for an email from NetBeacon asking you to confirm your email address.

OKAY

An administrator has created an account for you at NetBeacon. Please [confirm your account](#). This confirmation link is only valid for the next 30 minutes.

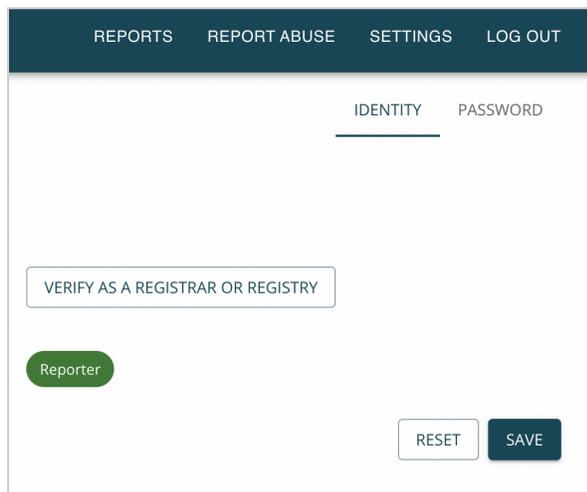
Notice

Your email has been verified. You may now log in.

OKAY

#### 4. Claim Your Registrar

- a. Click Settings
- b. Under Identity
- c. Click Verify as a Registrar or Registry



- d. Select your Registrar from the drop down, read the Terms of Use, agree to the Terms of Use, and click Confirm

**Request Verification**

Select the registry or registrar you represent to request verification.

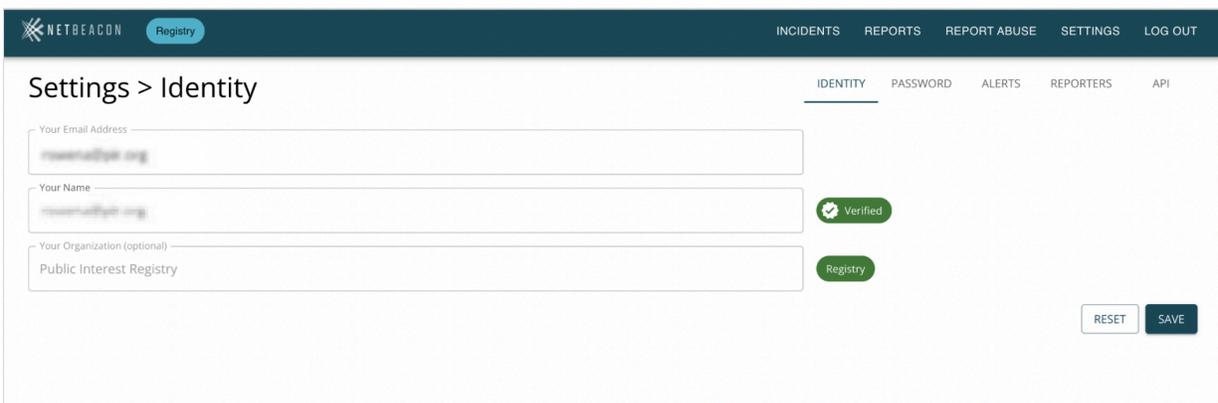
Registrar  Registry

Registrar Name \*

I have read and accept the [Recipient Terms of Use](#).

CANCEL CONFIRM

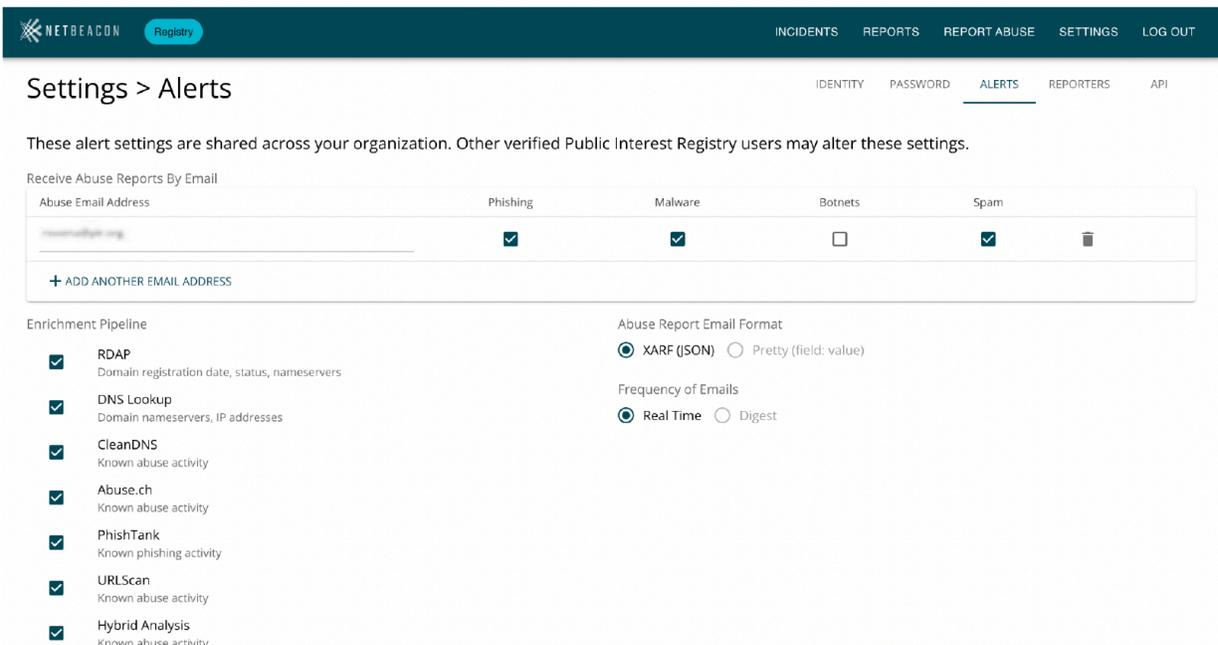
- e. This will need to be verified by a NetBeacon Reporter administrator. Once this has been completed, you will see green verification badges



The screenshot shows the 'Settings > Identity' page in the NetBeacon Reporter interface. The page has a dark blue header with the NetBeacon logo and 'Registry' tab. The main content area has a white background with a dark blue navigation bar containing 'INCIDENTS', 'REPORTS', 'REPORT ABUSE', 'SETTINGS', and 'LOG OUT'. Below the navigation bar, there are tabs for 'IDENTITY', 'PASSWORD', 'ALERTS', 'REPORTERS', and 'API'. The 'IDENTITY' tab is active. There are three input fields: 'Your Email Address' (containing 'rosemary@ipm.org'), 'Your Name' (containing 'rosemary@ipm.org'), and 'Your Organization (optional)' (containing 'Public Interest Registry'). To the right of the 'Your Name' and 'Your Organization' fields are green verification badges: a 'Verified' badge with a checkmark icon and a 'Registry' badge. At the bottom right, there are 'RESET' and 'SAVE' buttons.

# 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



The screenshot shows the 'Settings > Alerts' page in the NetBeacon interface. The top navigation bar includes 'INCIDENTS', 'REPORTS', 'REPORT ABUSE', 'SETTINGS', and 'LOG OUT'. The 'Alerts' sub-tab is active. Below the navigation, a message states: 'These alert settings are shared across your organization. Other verified Public Interest Registry users may alter these settings.'

**Receive Abuse Reports By Email**

Abuse Email Address	Phishing	Malware	Botnets	Spam	
<input type="text" value="example@pi.registry"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="🗑️"/>
<a href="#">+ ADD ANOTHER EMAIL ADDRESS</a>					

**Enrichment Pipeline**

- RDAP**  
Domain registration date, status, nameservers
- DNS Lookup**  
Domain nameservers, IP addresses
- CleanDNS**  
Known abuse activity
- Abuse.ch**  
Known abuse activity
- PhishTank**  
Known phishing activity
- URLScan**  
Known abuse activity
- Hybrid Analysis**  
Known abuse activity

**Abuse Report Email Format**

XARF (JSON)  Pretty (field.value)

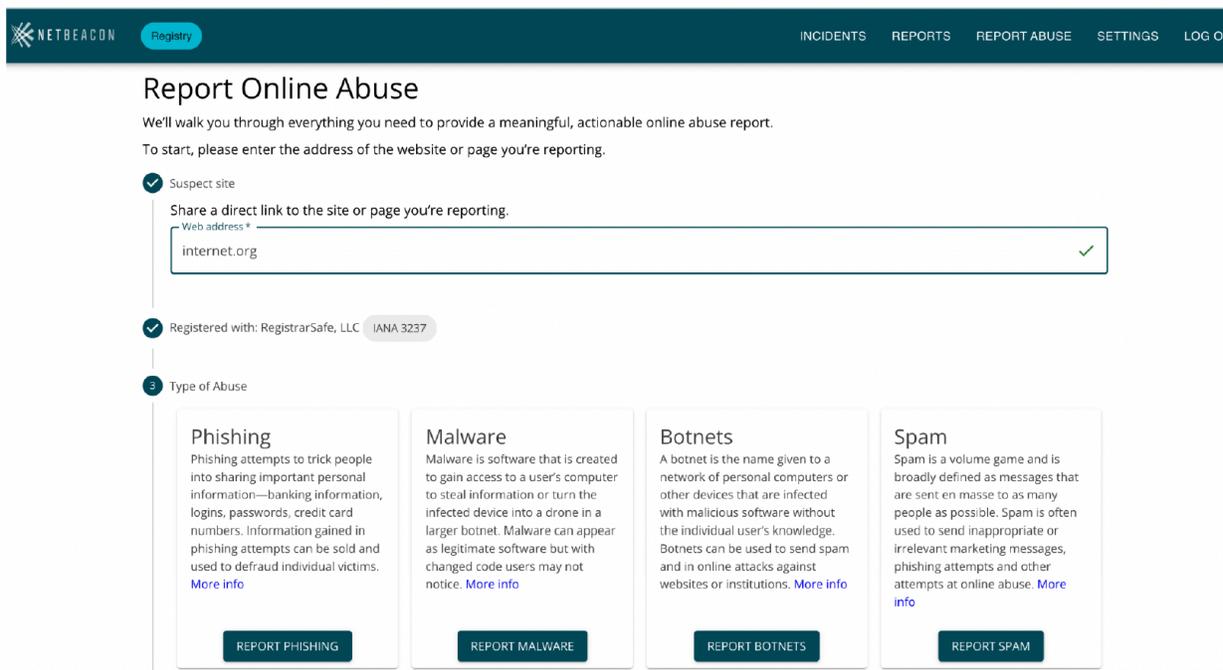
**Frequency of Emails**

Real Time  Digest

# 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)

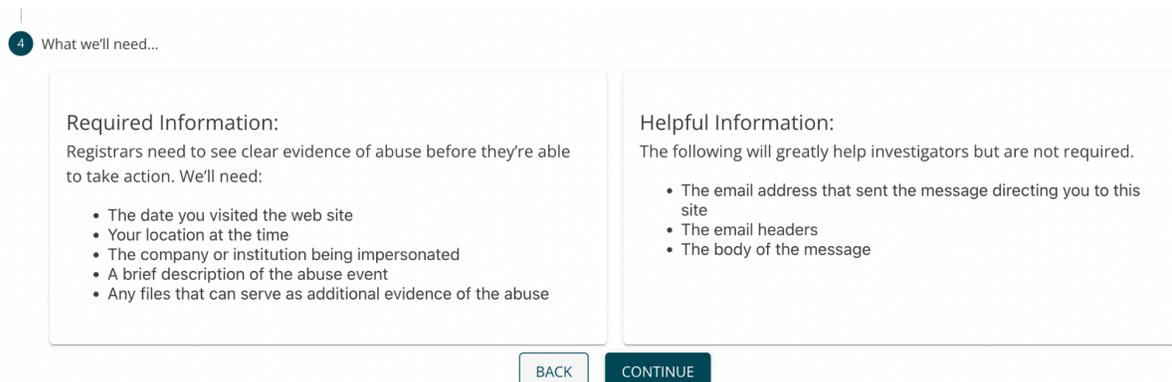


The screenshot shows the 'Report Online Abuse' form. At the top, there is a navigation bar with 'NETBEACON Registry' on the left and 'INCIDENTS', 'REPORTS', 'REPORT ABUSE', 'SETTINGS', and 'LOG O' on the right. The main heading is 'Report Online Abuse'. Below the heading, there is a sub-heading: 'We'll 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.'

The form has three steps:

- 1. Suspect site**: A section with a checkmark icon. It says 'Share a direct link to the site or page you're reporting.' Below this is a text input field labeled 'Web address \*' containing 'internet.org' and a green checkmark icon on the right.
- 2. Registered with: RegistrarSafe, LLC | IANA 3237**: A section with a checkmark icon.
- 3. Type of Abuse**: A section with a checkmark icon. It contains four cards:
  - Phishing**: Description: 'Phishing attempts to trick people into sharing important personal information—banking information, logins, passwords, credit card numbers. Information gained in phishing attempts can be sold and used to defraud individual victims. [More info](#)' Button: 'REPORT PHISHING'
  - Malware**: Description: 'Malware is software that is created 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](#)' Button: 'REPORT MALWARE'
  - Botnets**: Description: '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](#)' Button: 'REPORT BOTNETS'
  - Spam**: Description: 'Spam is a volume 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](#)' Button: 'REPORT SPAM'

4. Note the required information
5. Click Continue



The screenshot shows the 'What we'll need...' form. It has a step indicator '4' and a title 'What we'll need...'. The form is divided into two columns:

- 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
- 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

At the bottom of the form, there are two buttons: 'BACK' and 'CONTINUE'.

## 6. Enter the required information

## 7. Click Submit Report

1 Date of Incident  
The date you visited the web site.

2 Your Location  
Your geographic location at the time of the incident.

3 Institution Targeted  
The name of the company being impersonated.

4 Sender Email  
Provide the email address that sent the phishing message.

5 Message Headers and Body  
Provide the email headers and the body of the message.

6 What Happened?  
Provide a brief description of the abuse event.

7 Additional Evidence  
Share any files (e.g. screenshots) that might help.

8 Submit Report  
Your report is complete and can be submitted. By submitting this report, you consent to being contacted by a registry or registrar in the event that additional information is needed to act upon your abuse report.

BACK SUBMIT REPORT

## 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 752f42, 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

NETBEACON Registry

INCIDENTS REPORTS REPORT ABUSE SETTINGS LOG OUT

< BACK TO MY REPORTS

ABUSIVE URL	internet.org		REPORT ID	752f42
ABUSE TYPE	ABUSE DATE	ABUSE ONGOING	REPORTED AT	6/1/2022, 11:43:41 AM
Phishing	6/1/2022	Yes		

ABUSE DESCRIPTION  
test

PHISHING TARGET  
Internet

SUPPORTING EVIDENCE (1 FILE)

Report Online Abuse

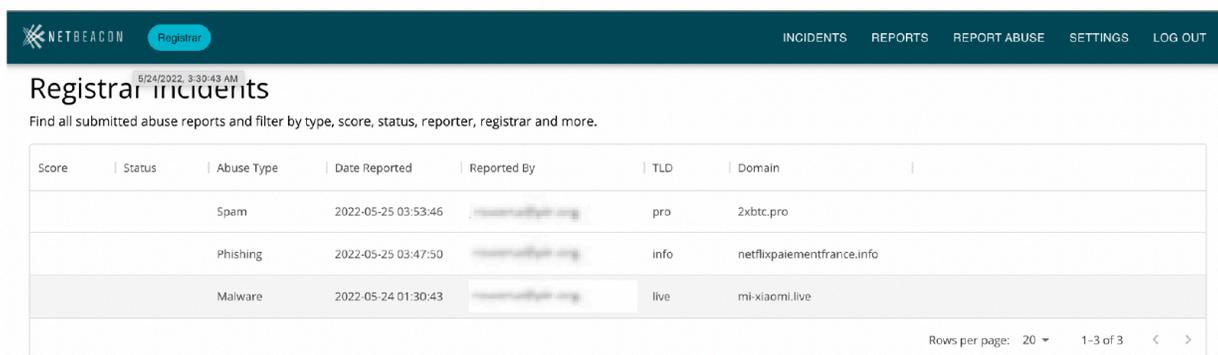
Phishing Malware Botnets Spam

# 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.

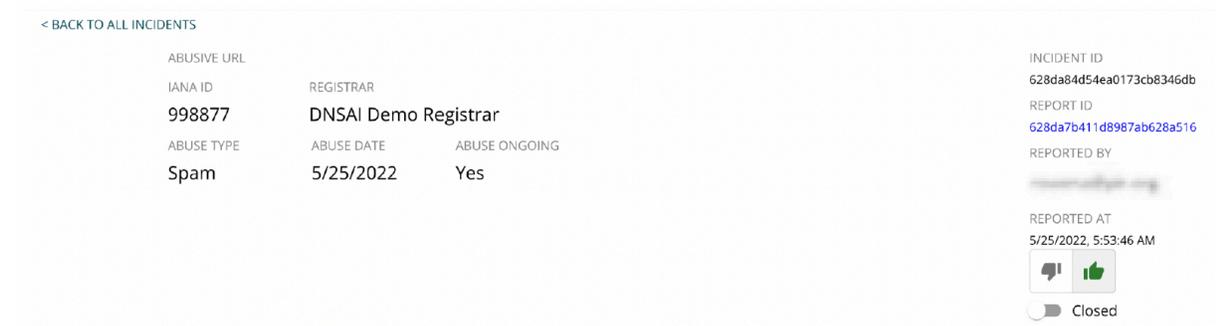
## 1. Navigate to Incidents in the top right menu



Score	Status	Abuse Type	Date Reported	Reported By	TLD	Domain
		Spam	2022-05-25 03:53:46	<a href="#">[redacted]</a>	pro	2xbtc.pro
		Phishing	2022-05-25 03:47:50	<a href="#">[redacted]</a>	info	netflixpaiementfrance.info
		Malware	2022-05-24 01:30:43	<a href="#">[redacted]</a>	live	mi-xiaomi.live

Rows per page: 20 | 1-3 of 3

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.



< BACK TO ALL INCIDENTS

ABUSIVE URL	REGISTRAR	
IANA ID	DNSAI Demo Registrar	
ABUSE TYPE	ABUSE DATE	ABUSE ONGOING
Spam	5/25/2022	Yes

INCIDENT ID  
628da84d54ea0173cb8346db

REPORT ID  
[628da7b411d8967ab628a516](#)

REPORTED BY  
[\[redacted\]](#)

REPORTED AT  
5/25/2022, 5:53:46 AM

Closed

# 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.

