Effective DNS Abuse Reports

This document draws on the Contracted Parties House Guide to Abuse Reporting Practices for evidentiary requirements and is a companion piece to this updated Abuse Reporting Guide, and this Reporting Online Harms flow chart.

This document also uses the percent symbol (%) to denote where the information in that position is variable.

Report Email Subject

If the report is submitted via email, the email subject should be:

- %type of harm% - %domainname[.]tld% - Reported by %Organization% (if applicable)

For example:

- Phishing - naughtyphishingdomain[.]tld - Reported by NetBeacon Institute
- Malware - badmalwaresite[.]tld

Information Ordering

Information in abuse reports should follow the following order:

1. Information about the abuse
2. Information about the domain
3. Information about who is reporting the abuse
4. Information about any evidence or attachments

Effective DNS Abuse Reports

Required and Optional Elements about the Abuse

Below is a table with the minimum required elements, as well as some common optional elements.

Element	Type	Required / Optional	Description
ABUSE DETAILS			
Domain Name	Field	Required	The defanged domain name in question
URL	Field	Required	The full defanged URL for the issue being reported
Abuse Type	Field	Required	The type of abuse, typically phishing, malware, botnets, or spam
Description	Field	Required	A short description of the issue. Generally no more than two or three sentences
Targeted Entity	Field	Dependent on Abuse Type	If phishing, the institution being impersonated, including their website
Date & Time Last Observed	Field	Required	The date and time the issue was most recently observed in UTC or with timezone
Verification Requirements	Field	Required	Any information required to verify the abuse in question. Most commonly: if a mobile browser is required, or if only viewable from a specific geographic location
Issue ID	Field	Optional	A unique ID for referring to the issue
DOMAIN			
Days Since Registration	Field	Optional	The # of days since the domain was registered
Name Servers	Field	Optional	The Nameservers currently attached to the domain
DNS Records	Field	Optional	Available DNS Records
Matching Domains	Field	Optional	A list of abusive domains, at this registrar, for which **all** of the corresponding evidence is the same.

Effective DNS Abuse Reports

Required and Optional Elements about the Report

Below is a table with the minimum required elements, as well as some common optional elements.

Element	Type	Required / Optional	Description
REPORTER			
Reporter Name	Field	Required	Name of abuse report submitter
Reporter Email	Field	Required	Email address of abuse report submitter
Organization	Field	Optional	Organization of abuse report submitter
Organization Website	Field	Optional	Website of the organization of the abuse submitter
EVIDENCE			
Email Headers	Field	Required if abuse involved email	Email headers from abusive email
Email Body	Field	Required if abuse involved email	The body of the abusive email
Screenshot(s)	Field	Required	Screenshots should a) capture the alleged abuse and b) contain either the browser address bar with the full URL visible, or be watermarked with the date and time of the screenshot, as well as the URL captured.
Attachment Description	Field	Required if attachment present	Short description of attached file.

Effective DNS Abuse Reports

Example Report with Minimum Fields

Email Subject: Phishing - capitalistexplotation-support[.]tld - Reported by NetBeacon Institute

Issue Summary

Domain Name: capitalistexplotation-support[.]tld
URL: hxxps://capitalistexplotation-support[.]tld/fakeloginpage
Abuse Type: Phishing
Description: I received a phishing email asking me to update financial information, the email linked to a fake banking website impersonating the Bank of Capitalist Exploitation.
Targeted Entity: Bank of Capitalist Exploitation - bce.tld
Date Last Observed: Fri Dec 09 2022 00:00:00 GMT+0000 (UTC)
Verification Requirements: None

Reporter

Reporter Name: Jane Doe
Reporter Email: jane@domain.tld

Incident Evidence

Attachment Description: Screenshot of impersonating website including attempt to capture login credentials

Effective DNS Abuse Reports

Example Report with Optional Fields

Email Subject: Phishing - capitalistexplotation-support[.]tld - Reported by NetBeacon Institute

Issue Summary

Domain Name: capitalistexplotation-support[.]tld
URL: hxxps://capitalistexplotation-support[.]tld/fakeloginpage
Abuse Type: Phishing
Description: I received a phishing email asking me to update financial information, the email linked to a fake banking website impersonating the Bank of Capitalist Exploitation. Included in this report is both the email and a screenshot of the website.
Targeted Entity: Bank of Capitalist Exploitation - bce.tld
Date Last Observed: Fri Dec 09 2022 00:00:00 GMT+0000 (UTC)
Verification Requirements: Mobile browser, in Canada
Sender Email Address: noreply@id9330033.capitalistexplotation-support[dot]tld
Incident ID: 6393b942e80e2b26c09697d8

Domain Information

Days Since Registration: 3
Nameservers: ns1.totallynaughtyhost.tld, ns2.totallynaughtyhost.tld

Reporter

Reporter Name: Jane Doe
Reporter Email: jane@domain.tld
Organization: Doe Domain Catchers
Organization Domain: domain.tld

Incident Evidence

email headers: <bunch of email header text>
email body: <bunch of email body text>
Attachment Description 1 of 2: Screenshot of impersonating website
Attachment Description 2 of 2: Screenshot of phishing email