

CleanDNS

CleanDNS

Cleaning up the Internet for GOOD

The Enemy of Security is Convenience!

To facilitate a safer domain name system standardization and streamlining abuse remediation is essential.

Best Practices?

- The number of phishing attacks has tripled since May 2020 and has increased 65% over the previous yearly study period.
- The number of unique domain names reported for phishing continues to increase.
- More than 1 million unique domain names were reported for phishing during the current yearly period.¹

Many years of work and arguments later – appropriate action and expectations are being asserted:

- **Framework to Address Abuse** – <http://dnsabuseframework.org>
- **Internet and Jurisdiction Policy Framework** – DNS level Action to Address Abuse - <https://www.internetjurisdiction.net/domains/toolkit>
- **SAC 115 – Report on an Interoperable Approach**
<https://www.icann.org/en/system/files/files/sac-115-en.pdf>
- **ICANN's clarity of message and expectations have continued:** -
<https://www.icann.org/resources/press-material/release-2022-05-17->

Clear alignments on the appropriateness of action and the need for strong evidence

Emphasis is now on properly escalating **appropriately evidenced abuse** within appropriate thresholds, standards, and frameworks.

Today's Common Method: Report

1. Abuse Link

2. Provide Details

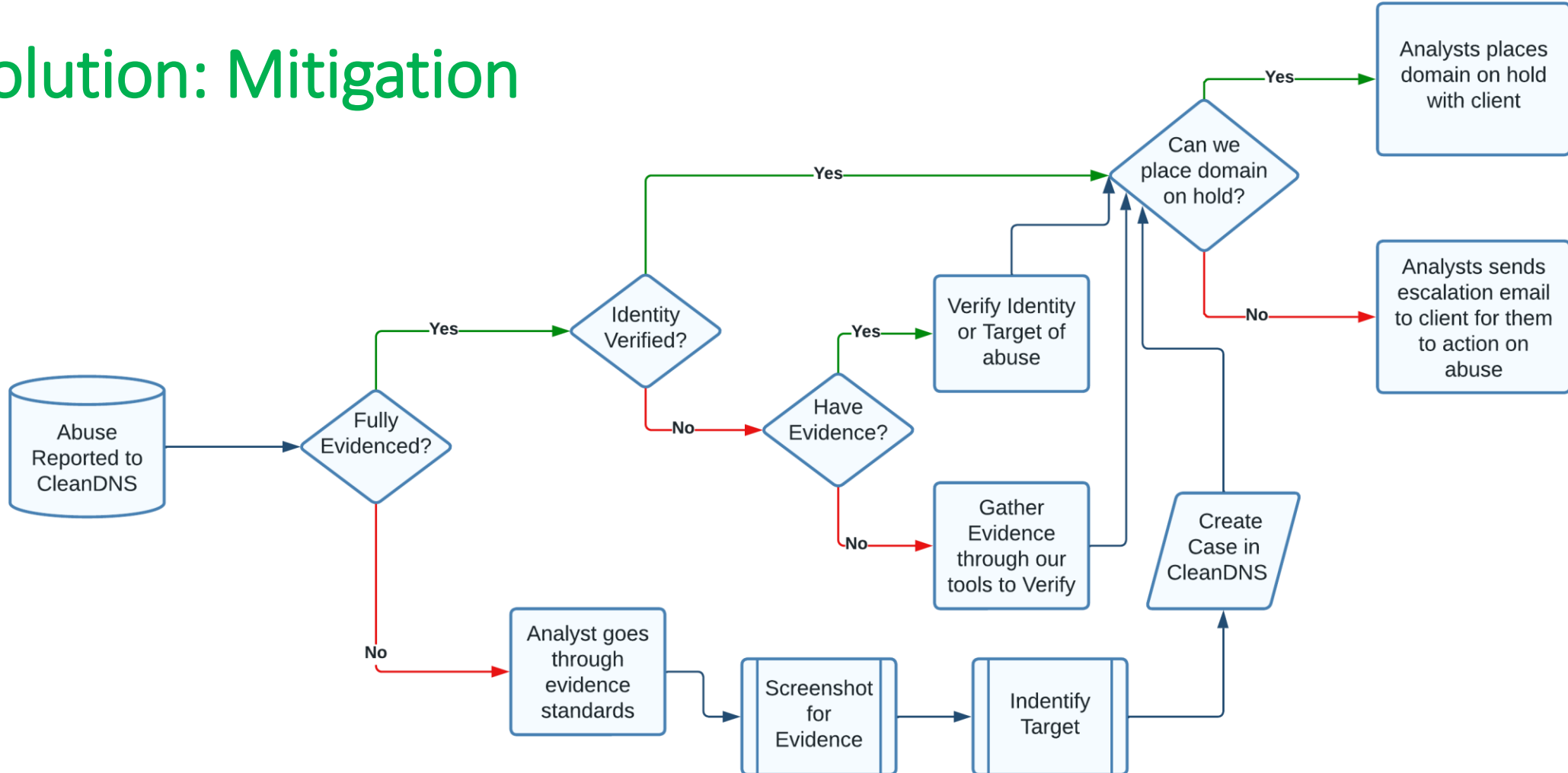
- Domain appears on an abuse list or is manually reported for abuse.
- Screenshot depicting a credential/ PII/ passphrase/ credit card input and/or QR code (for cryptocurrency).
- Redirects must include a Link Redirect Screenshot.
- **Financial Institution:* acceptable screenshot can include the institution's home page without an input for credentials.

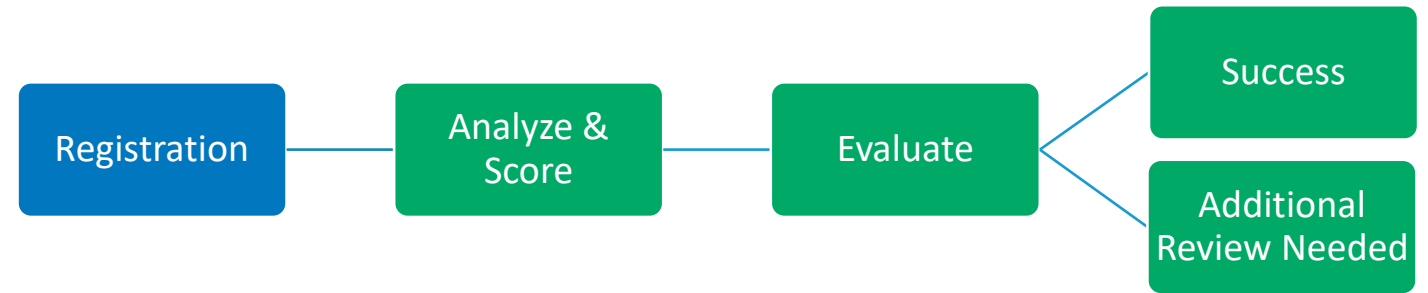
3. Submit

Report

Submit

Today's Solution: Mitigation





CleanDNS

Thank you!