

# Technical Means to Fight Phishing

## APTLD84 | Session 7B



**Pinky Brand**  
Senior Vice President  
iQ Global AS

# Is the domain benign or malicious?



How do you reach a verdict?

# Best Practices

## *from Policy to Procedures*



### Considerations:

- Who should be responsible for dealing with a phishing report?
- What types of phishing reports will you deal with?
- Define how you will act for different types of phishing reports or reporters
- How long will you wait before taking action?
- Monitoring your namespace for abusive phishing domains
- Staffing levels

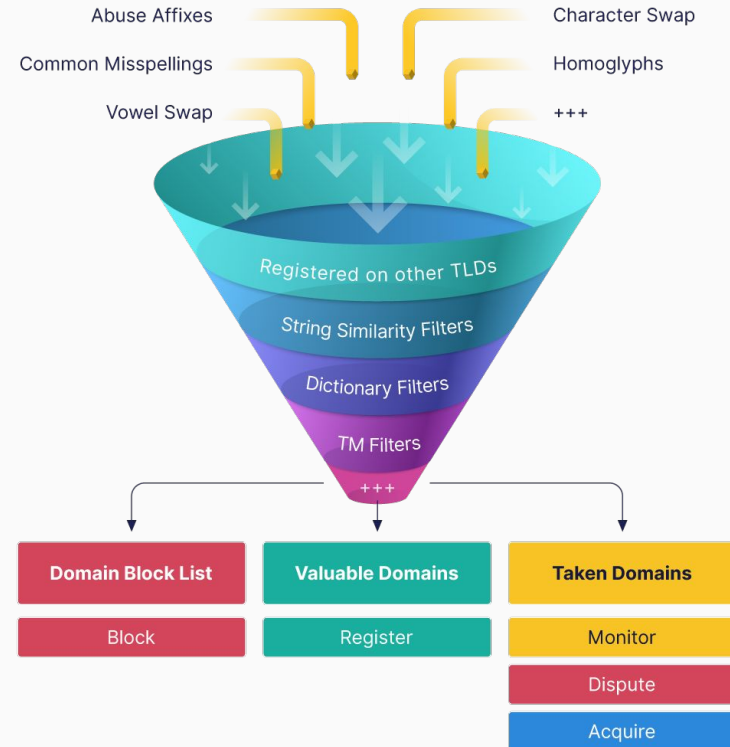
# One solution: Using data-driven tech and AI



The industry needs proactive blocking at scale to prevent domain name registrations used for phishing.

## The Challenge?

Registry level blocking without impacting registration revenue and your namespace



# Another solution: Domain Risk Scoring



Rate domain names  
for potential risk at any stage  
of the domain registration process

- Linguistic analysis
- String entropy analysis
- Typos and homoglyph analysis
- Trademark similarity
- Abuse affix analysis
- Domain property analysis
- DGA detection

The interface displays a search bar with the text "visa-login". To the right of the search bar is a red button labeled "Risk Score" and two toggle switches: "Abuse Lookup" and "TM Check", both of which are currently turned off. Below the search bar, the keywords "vis visa log logi login gin" are listed. The main content area is divided into two sections. The left section, titled "RISK SCORE", shows a score of "0.7" with a green circular icon containing a dollar sign. The right section, titled "RISK SCORE ALL WEIGHTS", shows a score of "0.53" with a similar green icon. Below these sections is a "Risk Score Results" section with a "Group by Algorithm" button. This section contains eight boxes, each representing a different risk factor: "ABUSE\_AFFIX", "CONSONANTS", "HYPHENS", "PERCENT\_NUMERIC", "PRONOUNCEABILITY", "SHANNON\_ENTROPY", "SLD\_EXACT\_MATCH\_TM", and "SLD\_STRINGS\_CONTAINS\_TM". The "STRING\_LENGTH" factor is also shown with a value of "10".

1

Domain Search

2

Checkout

3

Pre provisioning

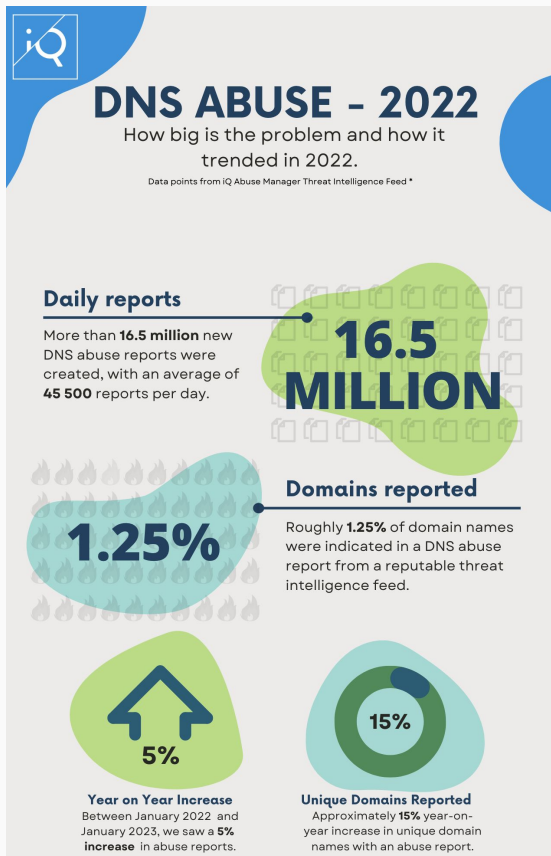
4

Post Provisioning

5

Historical Data

# FREE COMMUNITY RESOURCE: AbuseStats.com



**DNS ABUSE 2022 References:** Data points from iQ Abuse Manager Threat Intelligence Feed. Data composed from meticulously monitored and vetted abuse reports, from well-known providers such as the Anti-Phishing Working Group and Spamhaus. Covers the same sources as the ICANN DAAR and several more.

# Contact



Pinky Brand

pinky@iq.global

<https://iq.global>