

# Axur's DNS Abuse Overview

2025

 **AXUR**



# Who are we?



Axur is an external cybersecurity platform that protects businesses from threats outside the perimeter.

## Topics

- 01 Our DNS abuse overview
- 02 How we fight DNS abuse
- 03 Challenges & suggested solutions



# Our DNS abuse overview

## An average day at Axur

 **~16 million**  
URLs are analyzed

## An average day at Axur

 **~16 million**  
URLs are analyzed



 **~ 1 million**

URLs are inspected for fraud by our AI model



# +5 billion

URLs analyzed for potential  
DNS abuse by Axur in 2025



# +70 thousand

phishing pages were detected  
by us in 2025





# 70%

of phishing scams don't use the  
targeted victim keyword in the domain

 [https://www.\*\*company\*\*-website.com](https://www.company-website.com)



# 70%

of phishing scams don't use the  
targeted victim keyword in the domain

 [https://www.\*\*company\*\*-website.com](https://www.company-website.com)

# 18%

of phishing scams don't use the  
targeted victim keyword in the HTML

 `<span>company</span>`

# Detecting phishing with AI inspection

Screenshot

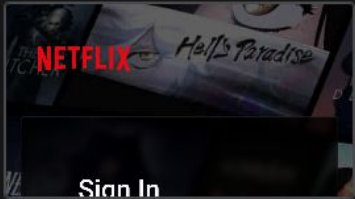





Image description

The image shows a login interface with a black background. at the top, there is a logo with the word 'netflix' in red. below, there are fields labeled 'email or phone number' and 'password' with a 'sign in' button. there is a checkbox labeled 'remember me' and a link 'need help?'. at the bottom, it mentions 'admin? access admin panel' and 'google recaptcha'.




Impersonated brand #1

Netflix High





Impersonated brand #2

Google Low





Companies mentioned #1

Netflix





Companies mentioned #2

Google





Company logos #1

Netflix






Company logos #2

Netflix





Content type

Login page



Predominant colors #1

Red (#DB1514 )



# Detecting phishing with AI inspection

Screenshot

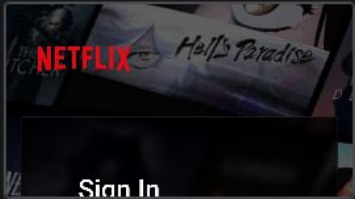





















Image description ✨ The image shows a login interface with a black background. at the top, there is a logo with the word 'netflix' in red. below, there are fields labeled 'email or phone number' and 'password' with a 'sign in' button. there is a checkbox labeled 'remember me' and a link 'need help?'. at the bottom, it mentions 'admin? access admin panel!' and 'google recaptcha'.

Impersonated brand #1 ✨	Netflix High			
Impersonated brand #2 ✨	Google Low			
Companies mentioned #1 ✨	Netflix			
Companies mentioned #2 ✨	Google			
Company logos #1 ✨	Netflix			
Company logos #2 ✨	Netflix			
Content type ✨	Login page			
Predominant colors #1 ✨	Red (#DB1514 )			

# Detecting phishing with AI inspection

Screenshot

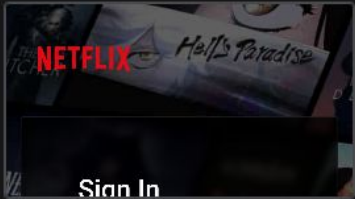


Image description

The image shows a login interface with a black background. at the top, there is a logo with the word 'netflix' in red. below, there are fields labeled 'email or phone number' and 'password' with a 'sign in' button. there is a checkbox labeled 'remember me' and a link 'need help?'. at the bottom, it mentions 'admin? access admin panel' and 'google recaptcha'.

Impersonated brand #1

Netflix High

Impersonated brand #2

Google Low

Companies mentioned #1

Netflix

Companies mentioned #2

Google

Company logos #1

Netflix

Company logos #2

Netflix

Content type

Login page

Predominant colors #1

Red (#DB1514 )

# Detecting phishing with AI inspection

Screenshot

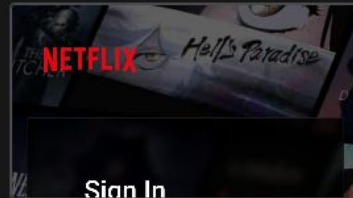


Image description

The image shows a login interface with a black background. at the top, there is a logo with the word 'netflix' in red. below, there are fields labeled 'email or phone number' and 'password' with a 'sign in' button. there is a checkbox labeled 'remember me' and a link 'need help?'. at the bottom, it mentions 'admin? access admin panel' and 'google recaptcha'.

Impersonated brand #1

Netflix High



Impersonated brand #2

Google Low



Companies mentioned #1

Netflix



Companies mentioned #2

Google



Company logos #1

Netflix



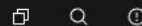
Company logos #2

Netflix



Content type

Login page



Predominant colors #1

Red (#DB1514 )



# AI makes creating and spreading fraud easier than ever

Threat Hunting

URLs & Domains




domain=lovable.app AND impersonatedBrandsHigh="Netflix"

For compliance reasons, searches are stored and may be monitored by Axur.

Edit columns

Export

Share

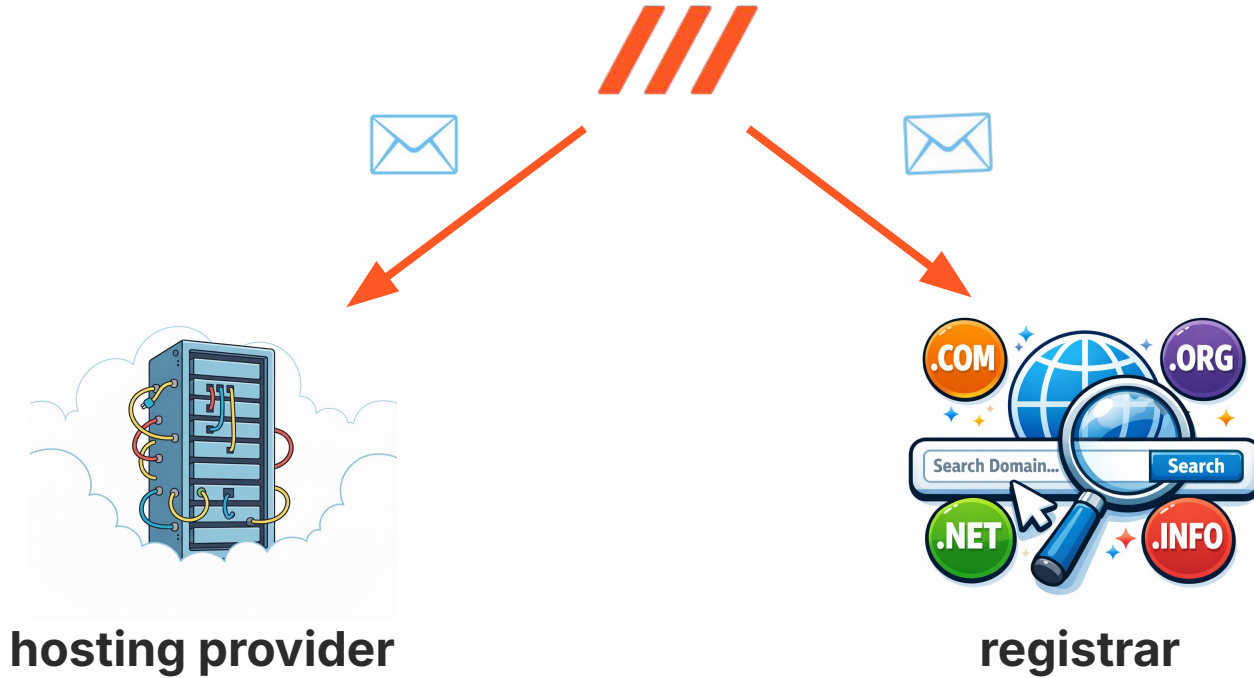
Detection date	Reference	Domain creation date	Screenshot	Content type	Impersonated brand
07/23/2025 at 02:33 AM	https://preview--netflix-auth-guardian.lovable.app/	05/06/2023 at 11:03 AM		Login page	Netflix - High Impersonation Google - Low Impersonation
05/19/2025 at 03:52 AM	http://flixreviewer.lovable.app	05/06/2023 at 11:03 AM		Other	Netflix - High Impersonation
05/19/2025 at 02:16 AM	https://flixreviewer.lovable.app/	05/06/2023 at 11:03 AM		Other	Netflix - High Impersonation



# How we fight DNS abuse



# We send notifications to responsible entities





**The takedown process works really well most of the time**



# The takedown process works really well most of the time

**+44 thousand**

phishings removed  
in 2025



# The takedown process works really well most of the time

**+44 thousand**

phishings removed  
in 2025

**98.79%**

phishing takedown  
success rate (YTD)



# The takedown process works really well most of the time

**+44 thousand**

phishings removed  
in 2025

**98.79%**

phishing takedown  
success rate (YTD)

**9.76 hours**

median uptime for  
phishings (YTD)



# Challenges & suggested solutions



Speed is critical for fighting DNS abuse





Speed is critical for fighting DNS abuse



Most victims fall within the first 24 hours





Speed is critical for fighting DNS abuse



Most victims fall within the first 24 hours



The financial impact and number of credentials stolen increase every hour



Speed is critical for fighting DNS abuse



Most victims fall within the first 24 hours



The financial impact and number of credentials stolen increase every hour



Attacks often happen at night and on weekends





Speed is critical for fighting DNS abuse



Most victims fall within the first 24 hours



The financial impact and number of credentials stolen increase every hour



Attacks often happen at night and on weekends



Therefore, automated takedown flows are essential for timely action

## Challenge 1: Barriers to Reporting Automation

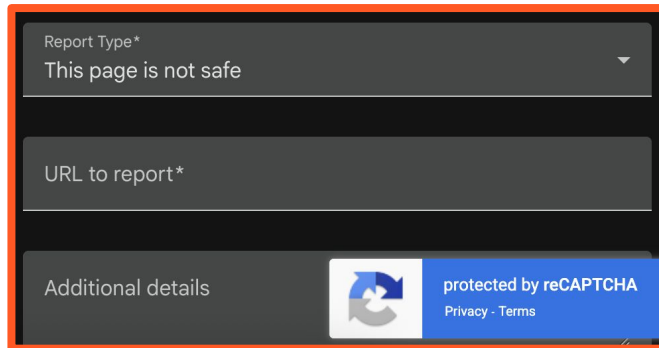
- Most report channels are publicly available, enabling anyone to report fraud

## Challenge 1: Barriers to Reporting Automation

- Most report channels are publicly available, enabling anyone to report fraud
- This openness is useful but sometimes exploited to spam entities with low-quality data

# Challenge 1: Barriers to Reporting Automation

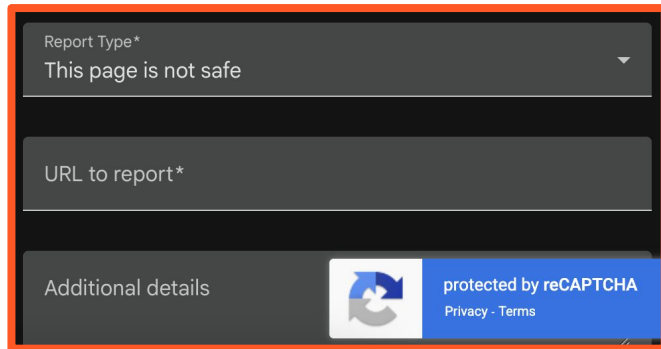
- Most report channels are publicly available, enabling anyone to report fraud
- This openness is useful but sometimes exploited to spam entities with low-quality data
- To address this, companies add automation barriers such as CAPTCHAs



Google safebrowsing report form

# Challenge 1: Barriers to Reporting Automation

- Most report channels are publicly available, enabling anyone to report fraud
- This openness is useful but sometimes exploited to spam entities with low-quality data
- To address this, companies add automation barriers such as CAPTCHAs
- These barriers reduce spam but complicate 24/7 automated reporting



Google safebrowsing report form



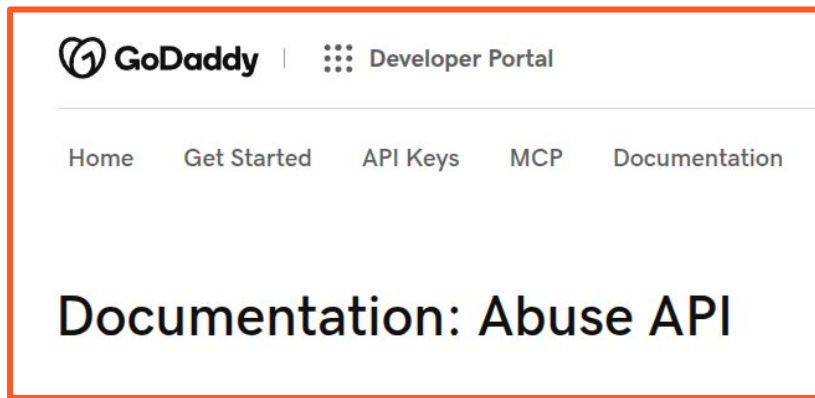
## Solution:

- Automation-friendly reporting channels with improved reporter identification



## Solution:

- Automation-friendly reporting channels with improved reporter identification
- A great example is registrars that offer an abuse API, such as GoDaddy and Namecheap



[GoDaddy Abuse API documentation](#)

## Challenge 2: Non-Compliant Entities

- In some cases, entities do not act in a timely manner - or do not act at all

## Challenge 2: Non-Compliant Entities

- In some cases, entities do not act in a timely manner - or do not act at all
- On the server side, there are so-called bulletproof hosting services



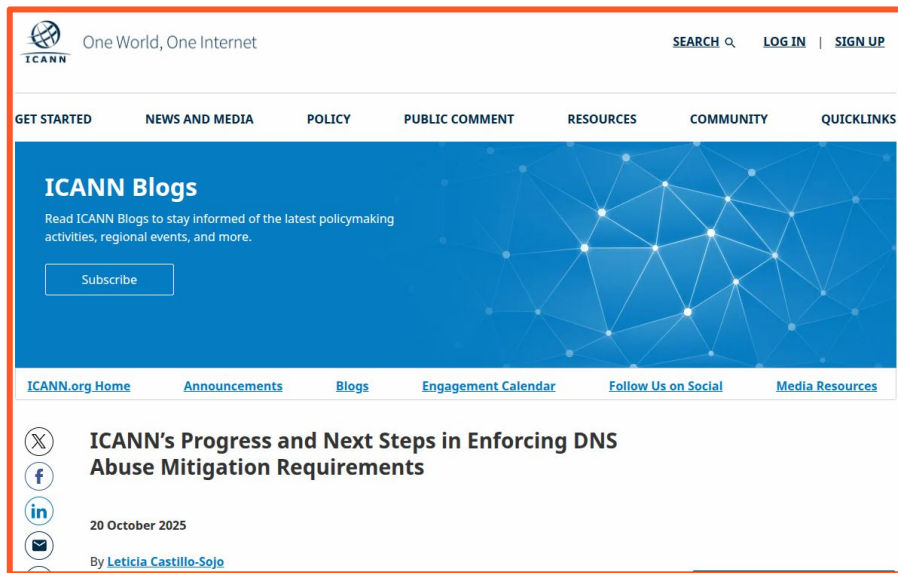
[Techradar, November 20, 2025](#)

## Solution:

- We rely on global law enforcement and internet backbone institutions such as ICANN

# Solution:

- We rely on global law enforcement and internet backbone institutions such as ICANN
- We are excited to learn about ICANN's work on the subject



[ICANN Blog 20 October 2025](#)



Thank you!

AXUR

