













CatPhish

CONFIDENTIAL. COPYRIGHT 2024, ALL RIGHTS RESERVED.
PHISHING TACKLE LIMITED

CatPhish Domain Monitoring

Monitoring	AI Generated Domain	Domain	Description	Risk: Score %
		phishingtack1e.com	Using the digit "1" instead of "l"	17%
		phishingtacke.com	missing the "l" at the end	17%
		phishingtacklè.com	Using "è" instead of "e"	18%
		phishingtàckle.com	Using "à" instead of "a"	18%
		phishingtackle.com	using "i" instead of "j"	18%

01 AI Generated Domains

We use AI to create domains to be monitored, based on your registered domain and in the same style as malicious actors.

02 DNS Monitoring

Constant monitoring of Whois and DNS records to watch what is being registered, and when.







03 Evidence Gathering

Automated gathering of evidence to submit with any abuse/take-down request.

04 Takedown Assistance

AI generated instructions on how to register an abuse complaint, or request a domain take-down. In addition, we automatically generate the email correspondence, citing relevant legislation and using your selected writing tone.

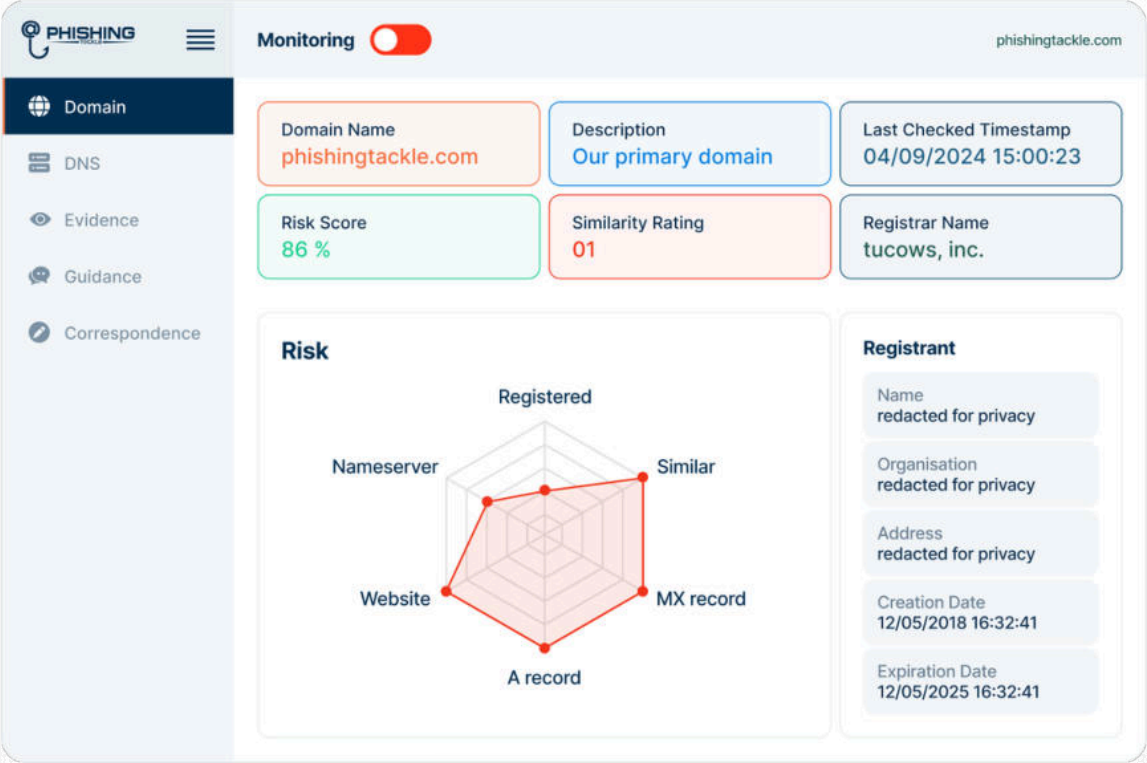
AI Generated Domain List

USE AI TO GENERATE SIMILAR DOMAIN NAMES				
Monitoring	AI Generated Domain	Domain	Description	Risk: Score %
		phishingtack1e.com	Using the digit "1" instead of "l"	17%
		phishingtacke.com	missing the "l" at the end	17%
		phishingtacklè.com	Using "è" instead of "e"	18%
		phishingtàckle.com	Using "à" instead of "a"	18%
		phishingtackle.com	using "i" instead of "l"	18%

The primary domain monitoring list as created by AI, based on your registered domains.

Here we can immediately see high risk domains.

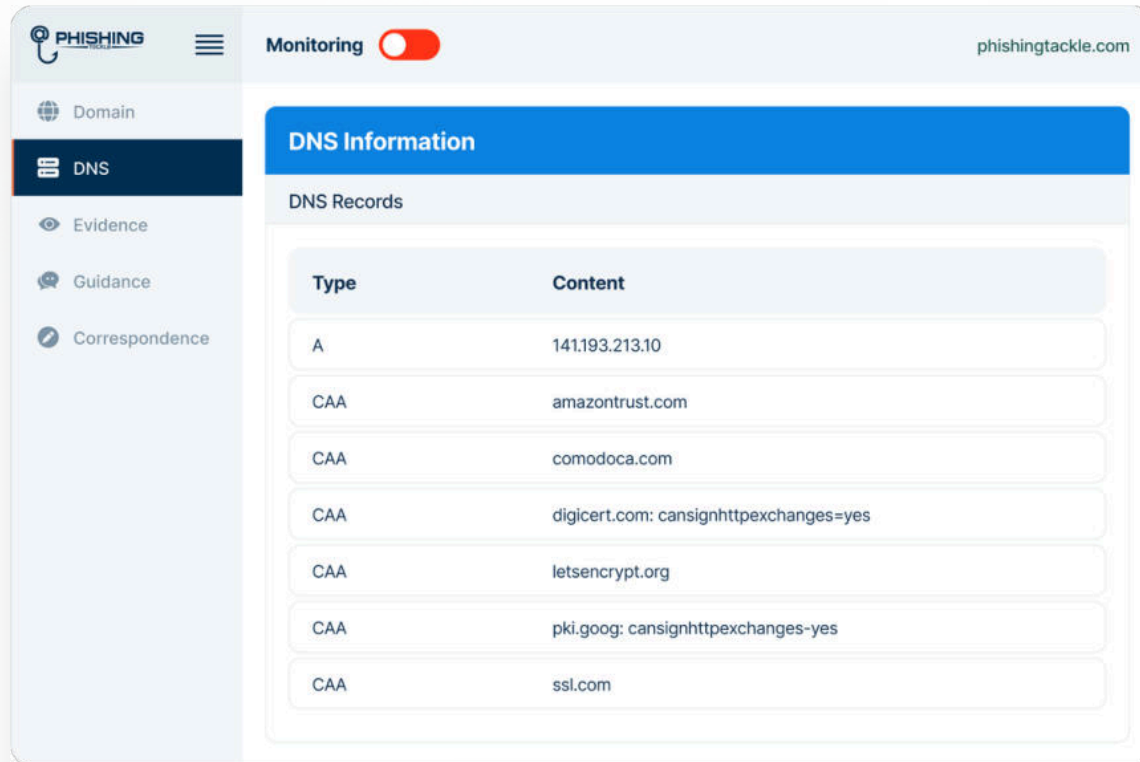
Domain Risk Overview



The domain risk overview page shows a summary of the registration of this domain.

We can see the overall risk score with the radar chart, and also other key information.

DNS Record Information



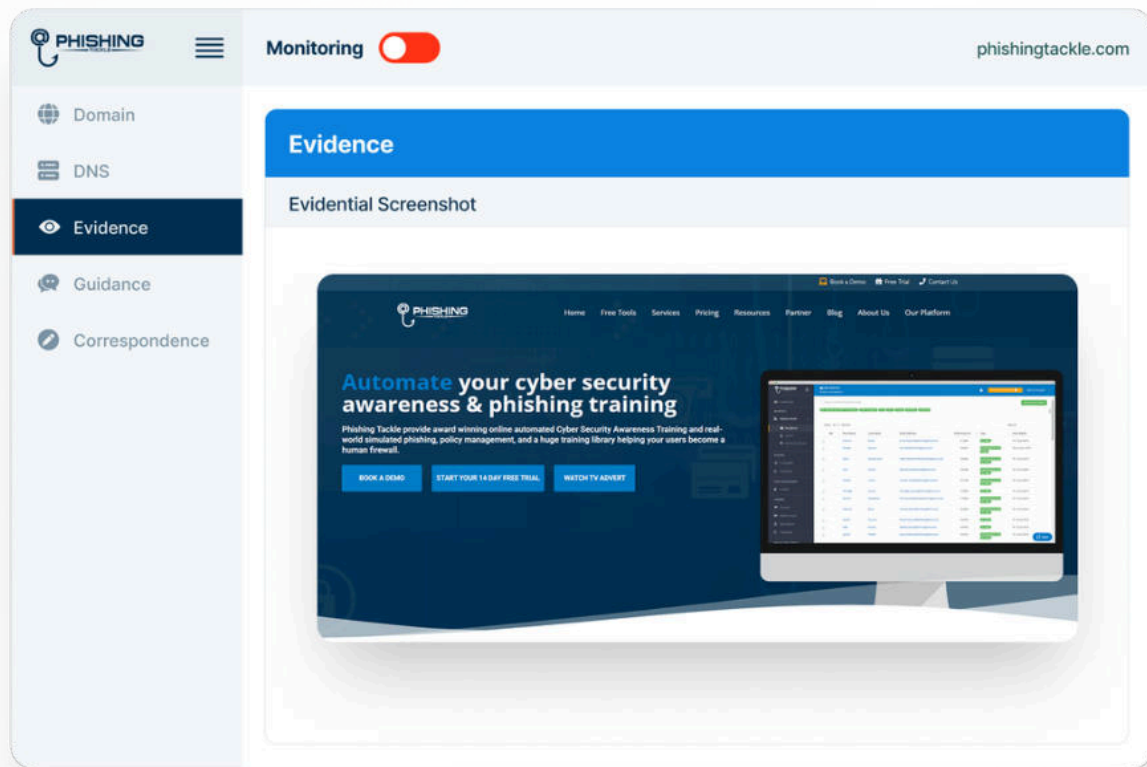
The screenshot shows the Phishing Tackle web application interface. On the left is a sidebar with navigation links: Domain, DNS (selected), Evidence, Guidance, and Correspondence. The top header includes the 'PHISHING TACKLE' logo, a menu icon, a 'Monitoring' toggle switch (which is turned on), and the URL 'phishingtackle.com'. The main content area is titled 'DNS Information' and contains a section for 'DNS Records'. This section displays a table with two columns: 'Type' and 'Content'.

Type	Content
A	141.193.213.10
CAA	amazontrust.com
CAA	comodoca.com
CAA	digicert.com: cansignhttpexchanges=yes
CAA	letsencrypt.org
CAA	pki.goog: cansignhttpexchanges=yes
CAA	ssl.com

Automated gathering of DNS information.

This is useful when understanding how far a malicious actor has gone to create an online persona for the potentially malicious domain.

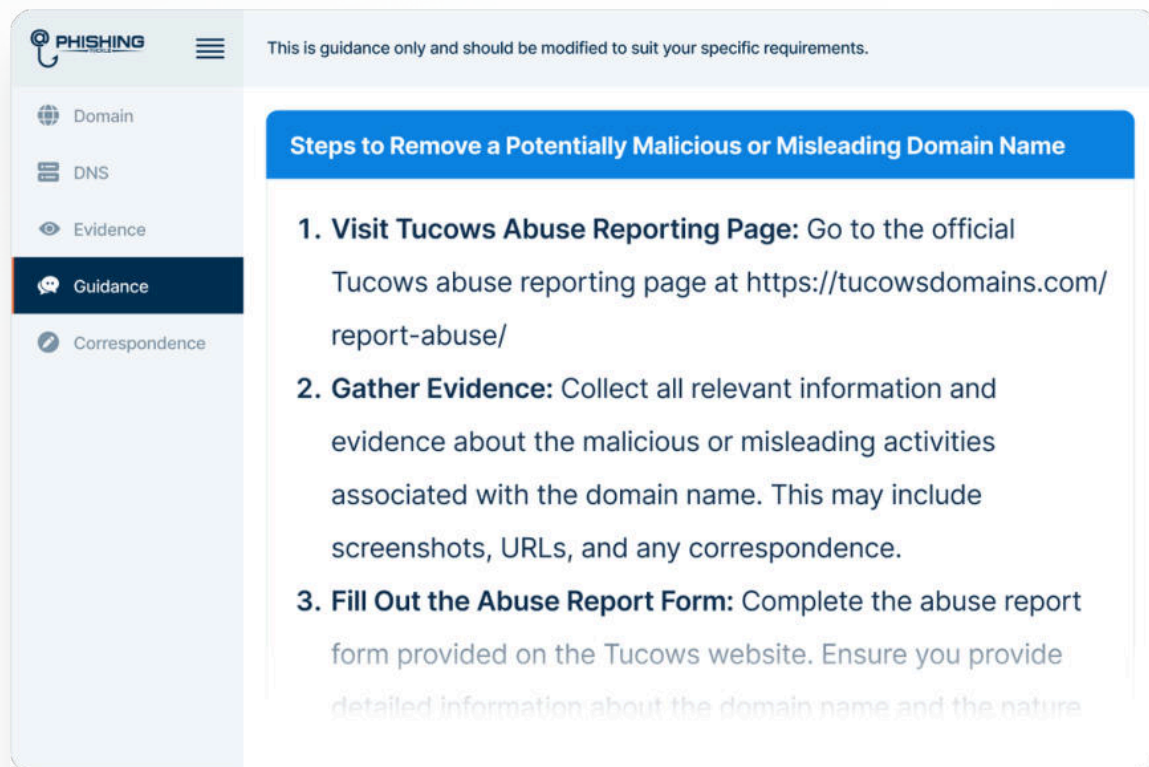
Domain Evidence



An evidential screenshot is automatically generated for the selected domain.

Having a working website behind a potentially maliciously registered domain is a strong indicator that it may be used to trick users into thinking it's genuine.


Registrar Abuse Process



The screenshot displays the PHISHING TACKLE website interface. On the left is a navigation sidebar with icons and labels for 'Domain', 'DNS', 'Evidence', 'Guidance' (which is highlighted with a dark blue background), and 'Correspondence'. The main content area has a light blue header with the text 'This is guidance only and should be modified to suit your specific requirements.' Below this is a blue banner with the title 'Steps to Remove a Potentially Malicious or Misleading Domain Name'. The content area lists three steps: 1. Visit Tu cows Abuse Reporting Page: Go to the official Tu cows abuse reporting page at <https://tu cowsdomains.com/report-abuse/>; 2. Gather Evidence: Collect all relevant information and evidence about the malicious or misleading activities associated with the domain name. This may include screenshots, URLs, and any correspondence; 3. Fill Out the Abuse Report Form: Complete the abuse report form provided on the Tu cows website. Ensure you provide detailed information about the domain name and the nature

Wherever possible, the registrar abuse details will be gathered and detailed instructions provided on how to register the abuse complaint.

Automated AI Generated Correspondence



Domain

DNS

Evidence

Guidance

Correspondence

This is guidance only and should be modified to suit your specific requirements.

Correspondence

ToneASCERTIVEJurisdictionUNITED KINGDOM

GENERATE CORRESPONDENCE

COPY CORRESPONDENCE

Subject: Concern Regarding the Domain "phishingtackle.com"

Dear Tucows Domains Inc. Team,

I am writing to express my concern regarding the domain "phishingtackle.com", which is registered under your organisation. Our company holds a similar domain name, and we are worried that this domain could potentially be used for malicious activities, either now or in the future.

As you may be aware, under the laws of the United Kingdom, including but not limited to the Computer Misuse Act 1990 and the Data Protection Act 2018, it is imperative to ensure that domains are not utilised for any fraudulent or harmful purposes. We believe that proactive measures should be taken to prevent any misuse of this domain.

Using AI, we generate the correspondence required to send to the domain registrar when opening an abuse claim.

The tone of the correspondence can be selected.

ASCERTIVE

Passive

Formal

Legal

Ascertainative

Aggressive

The jurisdiction to use for the relevant legislation.

United Kingdom

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States

Uruguay

Uzbekistan