



SHADOWSPOTTER | Phishing domain detection

Detect look-alike domains early, enrich the evidence, and alert your team before customers are exposed.

The phishing problem

Phishing often starts before the first malicious email lands: attackers register confusingly similar domains, request certificates, configure DNS, and launch fake login pages.

Shadowspotter gives defenders an early-warning layer by continuously watching public domain intelligence for brand-relevant patterns.

```
entity:domain fuzzy_domain:swissbanking
```

Domain	First Seen	Last Seen
swissbank.eu 91.195.241.232	Oct. 4, 2023, 8:08 a.m.	Oct. 4, 2023, 8:11 a.m.
swissbalancing.com 104.21.17.73 172.67.223.59 2606:4700:3033::ac43:d3b 2606:4700:3035::6815:1149	Sept. 25, 2023, 9:16 a.m.	Nov. 24, 2023, 9:44 a.m.
swissbankny.com 199.59.243.225	Dec. 16, 2023, 7:24 a.m.	Dec. 16, 2023, 7:24 a.m.
swissbankingcloud.com 168.119.43.205	Oct. 28, 2023, 3:43 a.m.	Oct. 28, 2023, 3:43 a.m.
swissupranking.com 83.136.251.38	Nov. 15, 2023, 2:12 a.m.	Nov. 15, 2023, 2:14 a.m.
swissbank.digital 3.64.163.50	Sept. 17, 2023, 6:28 a.m.	Sept. 29, 2023, 7:33 p.m.
swissbank.uk 3.64.163.50	June 5, 2023, 12:01 a.m.	Dec. 4, 2023, 7:14 p.m.

Example: fuzzy-domain search for look-alike domains.

Ideal for

- Security operations teams
- Brand protection teams
- Financial services and SaaS providers
- MSPs and MSSPs protecting customer brands

What Shadowspotter does

Shadowspotter is a domain intelligence platform for searching and correlating DNS, WHOIS, TLS certificate, domain and HTTP data. Any scoped search can become a continuous detection that runs in the background and triggers notifications when a new match appears.

For phishing detection, teams can watch brand-adjacent domains, certificates and pages as they appear, prioritize suspicious infrastructure with evidence, and move faster on blocking or takedown before attacks scale.

Phishing detection workflow

1. Model your brand risk

Build queries for brand names, look-alikes, typosquats, high-risk TLDs, registrar signals, name servers or page titles.

2. Monitor new signals

Save the query as a detection to continuously evaluate newly observed registrations and internet-wide data.

3. Get actionable alerts

Send email or webhook notifications with enriched DNS, WHOIS, certificate and HTTP context; Enterprise plans can also integrate alerts via API.

4. Respond faster

Block domains, start takedowns, open tickets, tune detections and reduce the window of customer exposure.

Where Shadowspotter delivers value

Use-case examples

- Newly registered look-alike or typo domains
- Certificates issued for brand-like domains
- Fake login pages using your brand in page titles, favicons or metadata
- Suspicious combinations of registrar, DNS provider, TLD and lexical features
- Repeat infrastructure patterns used across campaigns

Why teams choose it

- Flexible search language designed for domain intelligence
- Continuous detections instead of one-off lookups
- Correlated evidence across DNS, WHOIS, certificates and HTTP data
- Notifications via email or webhooks, plus API access on Enterprise plans
- Practical for small teams, brand protection programs and enterprise monitoring

Example detection ideas

```
entity:whois fuzzy_domain:yourbrand.com creation_date:2026-07-01+  
entity:http title:'*Your Brand*' NOT domain:*.yourbrand.com NOT domain:yourbrand.com
```

Start: shadowspotter.com

Contact: mail@shadowspotter.com

Takeaway: See first. Act faster.