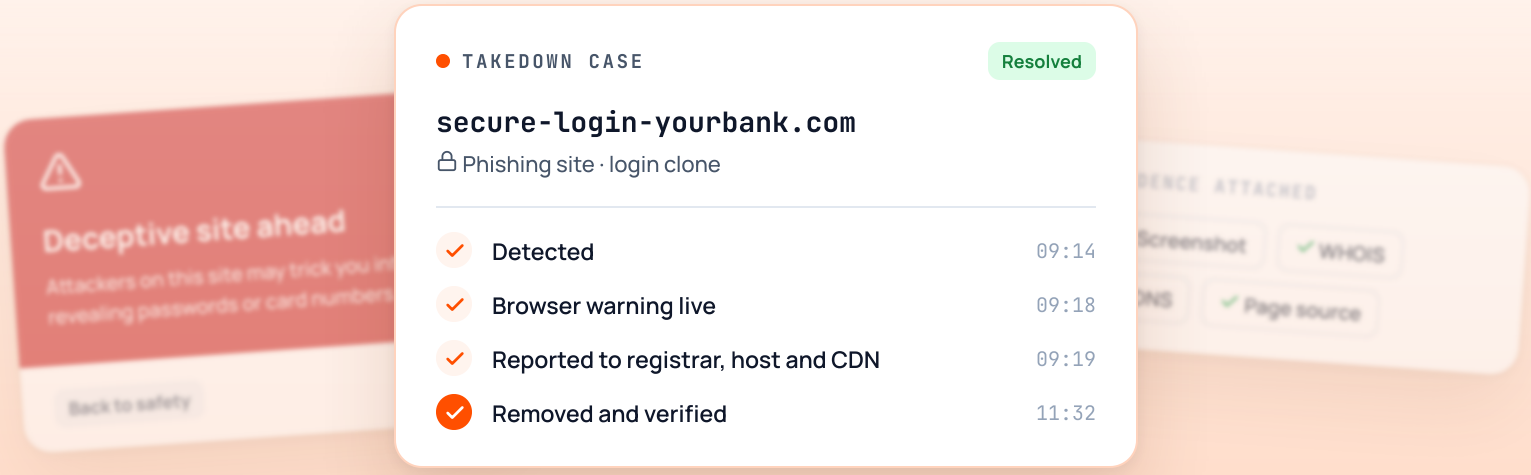
PHISHING TAKEDOWN PLAYBOOK

Flagged in minutes. Gone in days.

The Phishing Takedown Playbook.

The 14 steps, a report for every provider, and what to do when nobody answers.



CONTENTS

What's inside

Ten sections, from the first minutes to the final report. Work through it once to set up your process; during an incident, keep pages 4, 8 and 9 open.

01 **Why speed decides** p. 3
Two clocks: time to warning and time to removal.

02 **The 14 steps** p. 4
Every step of a takedown, and which can be automated.

03 **Confirm and capture** p. 5
Make sure it's phishing, and record it before it changes.

04 **Find who controls it** p. 6
Registrar, host, CDN or platform: who can do what.

05 **Warn browsers first** p. 7
One report that protects Chrome, Safari and Firefox users.

06 **Report templates** p. 8
Registrar, hosting provider and CDN versions.

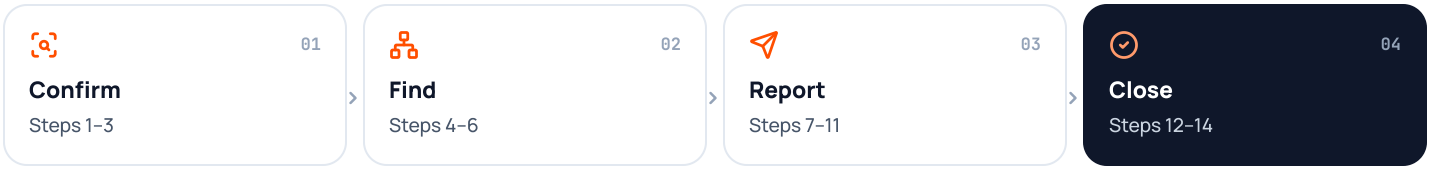
07 **Hard-to-reach hosts** p. 10
Cloudflare, Vercel, Netlify and other platforms.

08 **Follow up and escalate** p. 11
What to do when nobody answers.

09 **Choose the route** p. 12
Abuse reports, DMCA, URS and UDRP compared.

10 **Measure it** p. 13
The numbers that show phishing sites are actually gone.

FOUR PHASES, FOURTEEN STEPS



WHO THIS IS FOR

Security, SOC and fraud teams who handle phishing sites that copy their brand, and the agencies and MSSPs who do it for them. Nothing here needs special access: every route is open to any brand with evidence.

SECTION 01

01 Why speed decides

Most phishing sites do their damage in hours. A manual takedown takes days.

~60%

LIVE UNDER 10 MINUTES

of the phishing domains Google sees exist for less than ten minutes. By the time a manual takedown lands, most campaigns have moved on.

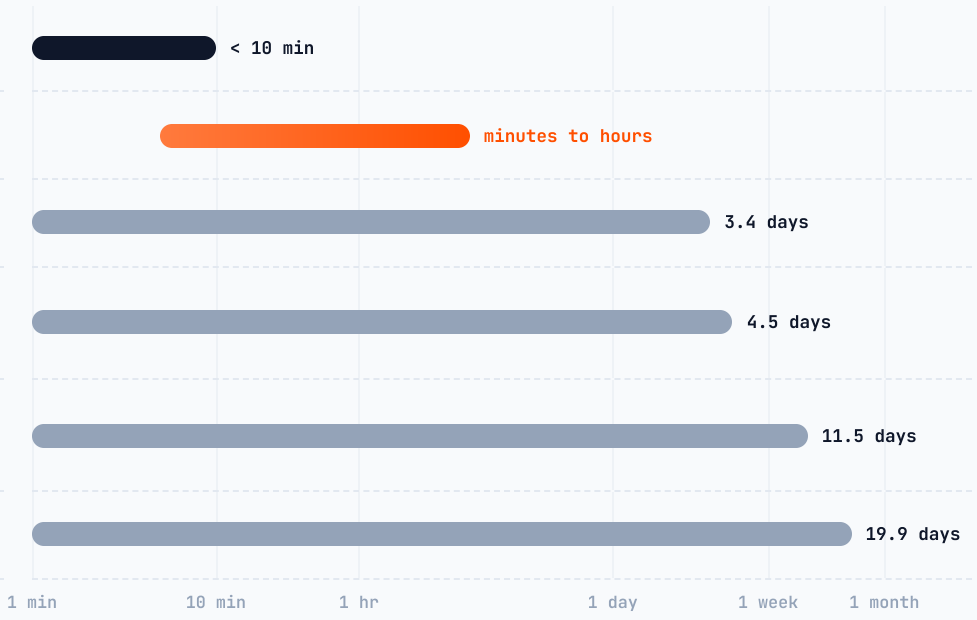
Source: The Hacker News, March 2024

Two clocks, not one

A takedown has two goals with different speeds: a browser warning protects most visitors within hours, and removal ends the harm for everyone. Track them separately, and start both the moment a site is confirmed.

THE GAP, DRAWN TO SCALE

Log scale



Sources: The Hacker News (2024), Cloudflare (2024), The Web Conference (2025), arXiv (2025). Full references on page 14.

RULE OF THUMB

Never run the steps in sequence

Report to Google Safe Browsing and to every provider on the same day. Waiting for the host before contacting the registrar gives the attacker time to move the page, and your first report is wasted.

SECTION 02

02 The 14 steps

Four phases. Almost every step is repetitive, which is why most can be automated.

01 Confirm

Is it phishing, is it live, what does it collect?

01 Confirm it's phishing

Check it imitates your brand and collects data

Mostly

02 Capture evidence

Timestamped screenshots, page source, the lure

Automatable

03 Check for cloaking

Load it from a phone, other countries and browsers

Automatable

02 Find

Who registered, hosts and fronts the site?

04 Look up the domain

RDAP: registrar, abuse contact, dates, nameservers

Automatable

05 Find the host

Resolve the IP; look up its owner and abuse contact

Automatable

06 Look behind the proxy

If a CDN fronts it, find the CDN and origin host

Partly

03 Report

Everyone who can warn or remove, the same day

07 Browser lists

Google Safe Browsing and Microsoft SmartScreen

Automatable

08 Registrar

Abuse report with evidence, asking for suspension

Automatable

09 Host

Same evidence, asking for removal

Automatable

10 CDN or platform

Its abuse form

Automatable

11 The lure

The email, SMS, ad or social platform that sent it

Partly

04 Close

Gone everywhere, and staying gone

12 Track tickets

Every report, ticket number and reply

Automatable

13 Follow up, escalate

Chase silent providers; registry, ICANN or CERT

Mostly

14 Verify and watch

Offline everywhere; watch for the same kit

Automatable

WHAT STILL NEEDS A PERSON

Unusual cases (a hacked legitimate site rather than a fake one), escalations that need a legal letter, and deciding when a domain is worth a UDRP.

SECTION 03 · STEPS 1–3

03 Confirm and capture

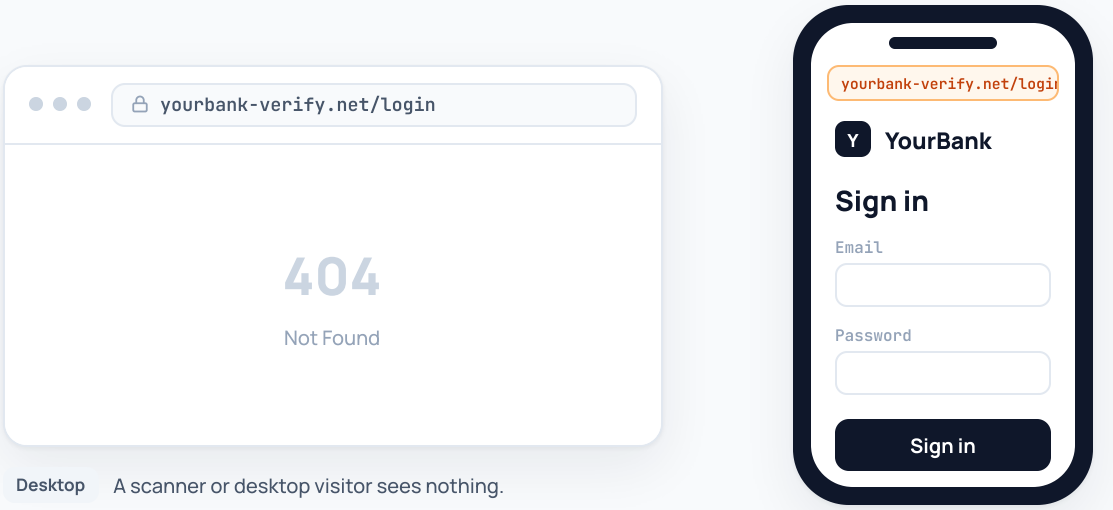
Before reporting anything, make sure it's phishing and record it. Phishing pages change and disappear fast.

Confirm three things

1. **It imitates your brand:** your name, logo, page layout or text.
2. **It collects something:** a password, a card number, a one-time code. That is the clearest sign of phishing.
3. **It is live now,** as your customers would see it.

CHECK FOR CLOAKING

Same address, two visitors



Desktop A scanner or desktop visitor sees nothing.

Phone A target on a phone sees the login clone.

Many phishing kits show the real page only to likely victims: a phone, a visitor from one country, anyone who isn't a known scanner. Capture what victims see, and say if it only shows for some visitors, or the reviewer may close the report.

CAPTURE THE EVIDENCE

Before it changes

- The **full URL** of the page, not just the domain
- The **page source**, or a HAR file
- Your **real page**, for comparison
- **Screenshots** with the date and time in UTC
- The **lure**: SMS, email with headers, ad or post
- How victims reach it; when first seen

Safety. Open suspected phishing pages in an isolated browser or virtual machine, never on a work laptop, and never enter real credentials.

SECTION 04 · STEPS 4–6

04 Find who controls it

A phishing site usually involves three or four companies, and each can do something different.

BETWEEN YOUR CUSTOMER AND THE PHISHING PAGE

	WHAT THEY CAN DO	HOW TO FIND THEM
Browser lists Safe Browsing, SmartScreen	**Warn** visitors while removal is pending	Google Safe Browsing and Microsoft SmartScreen report forms
CDN or proxy e.g. Cloudflare	**Forward** the report to host and owner; sometimes warn	The site's IP belongs to a CDN: use the CDN's abuse form
Platform Vercel, Netlify, Shopify…	**Remove** the site from its platform	The address is on the platform's domain: its abuse form
Hosting provider Owner of the IP	**Remove** the page and close the account	The IP's owner in its regional registry (ARIN, RIPE, APNIC, LACNIC, AFRINIC)
Registrar Sold the domain	**Suspend** the domain, so every page on it stops	The domain's RDAP record: "Registrar Abuse Contact Email" (lookup.icann.org)

If the IP belongs to Cloudflare or a similar service, that company is not the host: it forwards reports, so report to the CDN and, if you can find it, to the origin host directly. Proxies, privacy services and resellers mean the first contact you find is often not the one that can act.

WHOIS IS NOW RDAP

Since January 28, 2025, ICANN no longer requires registries of generic domains to run the old WHOIS service; registration data comes from RDAP. The registrar's abuse contact is still public, even when the owner's details are hidden.

2,700+

DOMAINS SUSPENDED

Since April 5, 2024, registrars of generic domains must act promptly on actionable evidence of phishing. In the first six months, ICANN opened 192 investigations under these rules, leading to more than 2,700 suspensions.

Source: ICANN, October 2024

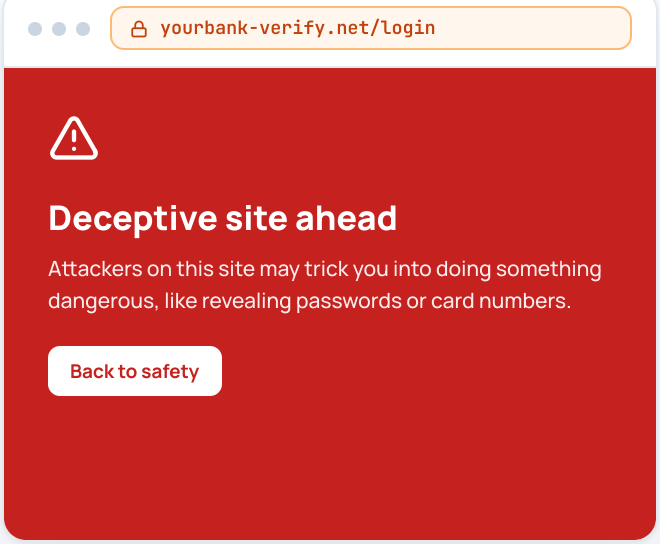
SECTION 05 · STEP 7

05 Warn browsers first

One accepted report to Google Safe Browsing puts a warning in Chrome, Safari and Firefox, about 88% of browsers in use.

ONE REPORT, MOST BROWSERS

Minutes to hours once accepted



BROWSERS THAT SHOW THE WARNING

~88% Edge, Opera, others

Chrome	Google Safe Browsing
Safari	Google Safe Browsing*
Firefox	Google Safe Browsing
Edge	Microsoft SmartScreen
Opera	Own lists, e.g. PhishTank

What gets a report accepted

- **The full address of the phishing page,** not the domain: the home page may look harmless.
- **A page that is live when the reviewer looks.** If it only appears on mobile or in one country, say so.
- **A form that collects something:** a password, a card number, a one-time code.
- **What it imitates,** with the address of your real page.
- **A screenshot with the date and time,** in case the page changes before review.

⚠ **A warning isn't a takedown.** The site is still online for anyone whose browser or app doesn't check the list, including some in-app browsers. Attackers can move the kit to a new address, and the warning doesn't follow. Report for removal on the same day. *Safari uses Tencent on devices set to mainland China; share from StatCounter.

SECTION 06 · STEPS 8–10

06 Report templates

Send the same evidence to every party at the same time. Replace everything in ‹angle brackets›.

1. Registrar: ask for suspension

New message · to the registrar's abuse contact

1 Subject: Phishing on <domain> impersonating <Brand>: request to suspend

To: <registrar abuse contact, from RDAP "Registrar Abuse Contact Email" or the registrar's abuse form>

We are reporting a domain registered through you that is being used for phishing. It impersonates <Brand> (<official domain>) and collects <account passwords / card details / one-time codes> from our customers.

2 Phishing URL (full address):
<https://domain/full/path>
First seen: <YYYY-MM-DD HH:MM UTC> Still live at: <YYYY-MM-DD HH:MM UTC>

What it imitates:
Our <login / checkout / support> page at <https://official URL>

3 Why it is phishing:
- It copies our <name, logo, page layout and text>
- It collects <what> through a form that sends the data to <where, if known>
- It is being sent to our customers by <SMS / email / ads / social posts> (sample attached)

Domain details:
Registered: <date> Nameservers: <ns1, ns2> Resolves to: <IP> (<network owner, ASN>)

4 Evidence attached:
1. Screenshot of the phishing page, <time UTC>
2. Screenshot of our official page, for comparison
3. <The lure message, with headers if it was an email>
4. <Page source or HAR file>

5 Requested action:
Please suspend <domain> under your abuse policy and your obligations to mitigate DNS abuse (phishing).

We are <the brand owner / an authorized representative of Brand>.
Contact: <name, role, email, phone>

1. **A subject that routes it**
Domain, brand and the action you want, so it lands in the abuse queue.

2. **The full address**
The page that collects data, with first-seen and still-live times in UTC.

3. **Why it is phishing**
What it copies, what it collects, and how victims reach it.

4. **Evidence**
Both screenshots, the lure and the page source.

5. **One clear request**
Suspension, citing its abuse policy and its **DNS abuse obligations**.

SECTION 06 · CONTINUED

2. Hosting provider: ask for removal

New message · to the host's abuse contact

```
1  Subject: Phishing page hosted on your network (<IP>) impersonating <Brand>

   To: <host abuse contact, from the IP's RIR record "abuse-mailbox" / "OrgAbuseEmail",
   or the host's abuse form>

   A phishing page impersonating <Brand> is hosted on your network.

2  Phishing URL (full address):
     <https://domain/full/path>
     Server IP: <IP>   First seen: <time UTC>   Still live at: <time UTC>

   What it imitates / why it is phishing / evidence:
     <same as the registrar report>

3  Requested action:
     Please remove the phishing content and suspend the account responsible.
     Please keep logs, in case they are needed by law enforcement.

   Contact: <name, role, email, phone>
```

1. **Name the network**
   Say the page is on their network, with the IP.
2. **Address and server**
   The full URL and the server IP, so they can find the account.
3. **Remove and keep logs**
   Removal, account suspension, and logs kept for law enforcement.

3. CDN or proxy (for example Cloudflare)

Use the provider's abuse form, choose the phishing category, paste the full URL and put the evidence summary in the description. A CDN usually doesn't store the site: it forwards your report to the host and the owner, so also report to the origin host if you can identify it.

BEFORE YOU SEND

- ✓ Full URL of the phishing page, re-checked live
- ✓ What it collects, and how victims reach it
- ✓ Reported to Safe Browsing and SmartScreen
- ✓ Screenshot with date and time (UTC), and our real page
- ✓ Sent to registrar, host and CDN at the same time
- ✓ Follow-up date set

SECTION 07

07 Hard-to-reach hosts

Proxies and serverless platforms change who you report to, and what you ask for.

PROXY OR HOST? IT CHANGES THE REQUEST

A proxy in front



The proxy doesn't store the site. Ask it to **forward and warn**, and report to the host behind it.

The platform is the host



The platform runs the site. Ask it to **remove the deployment** and suspend the account.

PROVIDER	ROLE	WHAT THEY CAN DO	IF NOTHING HAPPENS
Cloudflare (proxied site)	Proxy	Forward to host and owner, share the host contact, show a warning page	Report directly to the host it names; registrar of the domain
Cloudflare Pages / Workers	Host	Remove the site	Follow up on the same report; Google Safe Browsing
Vercel	Host	Remove the deployment	Follow up; registrar if it uses a custom domain
Netlify, GitHub Pages	Host	Remove the site or repository	Follow up; registrar if custom domain
Firebase Hosting (web.app)	Host	Remove the site	Google Safe Browsing

On a platform subdomain such as **acme-login-secure.vercel.app**, the platform owns the domain: no registrar will suspend it, and asking just delays your report. If it also has its own domain, report that to its registrar too.

WHAT THESE PROVIDERS NEED

- **The full address,** subdomain included: on a shared platform, it is the site
- **Proof it's live:** re-check and screenshot right before sending
- **The right request:** host removes, proxy forwards, registrar suspends

While you wait. Public threads show reporters waiting weeks on some platform reports. Make sure the address is on Google Safe Browsing and SmartScreen the same day, so visitors are warned while the platform reviews it.

SECTION 08 · STEPS 11–14

08 Follow up and escalate

This is where most of the hours go: some providers act within hours, others send an automated acknowledgement and nothing else.

When nobody answers

Next day — Follow up once
In the same thread, if the page is still live, with a fresh screenshot.

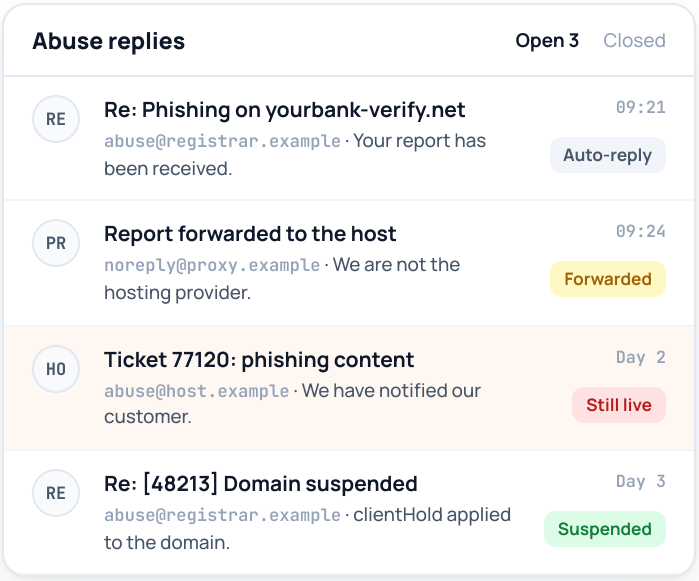
Then — Go one level up
The registry that runs the extension (Verisign for .com) has DNS abuse obligations too.

No action — Complain to ICANN
Its Contractual Compliance team takes complaints about registrars that don't act.

Same day — Report to shared feeds
APWG reports reach many security companies, registrars and hosts.

Persistent — Involve your CERT
Especially when the host is in another country.

What comes back



Illustrative. Fictional providers and domains.

Report the lure, too

The site needs visitors. Report the channel that sends them: the email provider, the SMS sender, the ad platform or the social network that delivered the link. Stopping the lure slows the campaign even before the site is gone.

CLOSE THE CASE PROPERLY

- Offline everywhere: every URL, from several countries and devices
- Watching for the same kit on new domains
- Evidence and correspondence kept with the case
- Closed only when removal is verified, not when the report was sent

SECTION 09

09 Choose the route

Abuse reports are the fastest route for a live phishing site. A UDRP is the only one that gives you the domain.



Which route for which situation

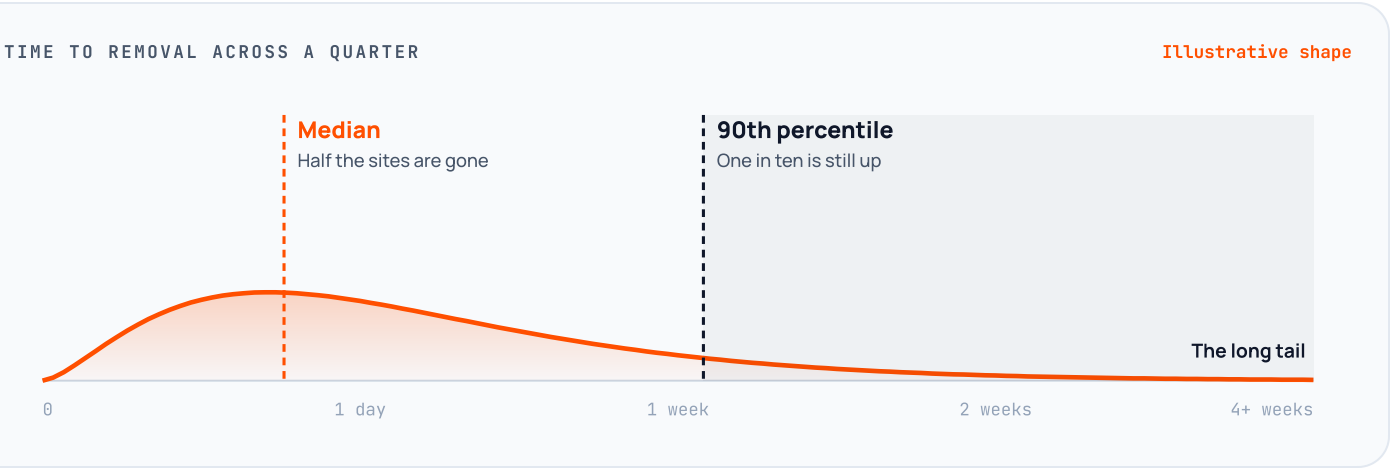
SITUATION	FIRST	THEN, IF NEEDED
Live phishing site on a lookalike domain	Abuse reports to host and registrar; Google Safe Browsing	UDRP if the domain keeps being reused
Your site copied onto an unrelated domain	Abuse report and DMCA notice to the host	Watch for the same copy
Phishing page on a platform subdomain	The platform's abuse form	Nothing to dispute
Parked lookalike with no content	Monitor it for signs of activation	UDRP or URS if bad faith is clear
Clear bad faith on a newer generic domain	URS for a quick suspension	UDRP to get the domain

⚖ **Not legal advice.** Talk to your lawyer before filing a UDRP, URS or DMCA claim. Run routes in parallel, never in sequence: file abuse reports the same day, and start a UDRP alongside them only if you want the domain.

SECTION 10

10 Measure it

Measure removed threats, not reports filed. Averages hide the sites that stay up for weeks.



METRIC	HOW TO MEASURE IT	WHY IT MATTERS
Time to warning	Confirmation → browser warning; median and 90th percentile	How fast most visitors are protected
Time to removal	Confirmation → offline, verified; median and 90th percentile	The number that ends the harm
Resolution rate	Share of cases offline and verified, not “reported”	A stalled case is still collecting data
Repeat rate	Same kit or operator back on a new domain	Campaigns or single sites?
Hands-on hours	Analyst time per takedown, by phase	The cost of doing it by hand

What doesn’t count

- ✕ **Reports filed** or **takedowns requested:** a report isn’t a removal.
- ✕ **Alerts:** finding a site protects nobody until it’s warned and removed.
- ✕ **An average on its own:** one site in ten staying up for weeks can look fine in the mean.

SET A BASELINE

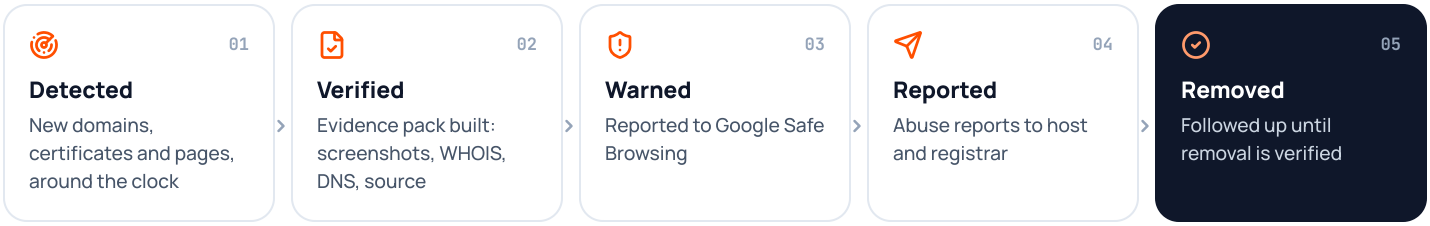
Measure your next ten takedowns

Record both clocks and the hands-on hours for each. That shows where the time goes and what to automate first.

HOW SENTRIKE HANDLES THIS

The playbook, run by AI agents

Sentrike runs each step of a takedown itself. Your team can follow every case; it doesn't have to do the work.



Sentrike's AI agents confirm the site is malicious, build the evidence pack, report it to Google Safe Browsing so Chrome, Safari and Firefox warn visitors within minutes, send abuse reports to the host and registrar, and follow up until the site is offline and removal is verified. Most sites are found before customers report them.

Stop chasing takedowns.

See the phishing sites using your brand today, and how fast they come down.

Request access →

sentrike.ai/takedown

SOURCES

Google introduces enhanced real-time URL protection for Chrome (The Hacker News, 2024) thehackernews.com/2024/03/google-introduces-enhanced-real-time.html

"7 days later": phishing site lifespan study (The Web Conference 2025) yonghwi-kwon.github.io/data/7_days_later_www25.pdf

Registration, Detection, and Deregistration: DNS abuse for phishing (arXiv, 2025) arxiv.org/pdf/2502.09549

Protecting Cloudflare sites from phishing (Cloudflare) blog.cloudflare.com/protecting-cloudflare-sites-from-phishing

2024 Global Amendments to the RAA and Registry Agreement (ICANN) www.icann.org/resources/pages/global-amendment-2024-en

ICANN's DNS Abuse Mitigation Program: key updates from 2024 (ICANN) www.icann.org/en/blogs/details/icanns-dns-abuse-mitigation-program-key

RDAP in 2025: the practical successor to WHOIS (NameSilo) www.namesilo.com/blog/en/domain-names/rdap-in-2025-the-practical-succe

Browser market share worldwide (StatCounter) gs.statcounter.com/browser-market-share

Vercel community thread on a phishing report community.vercel.com/t/urgent-request-to-suspend-a-phishing-website-ho

WIPO domain name dispute fees www.wipo.int/en/web/amc/domain-name-disputes/fees