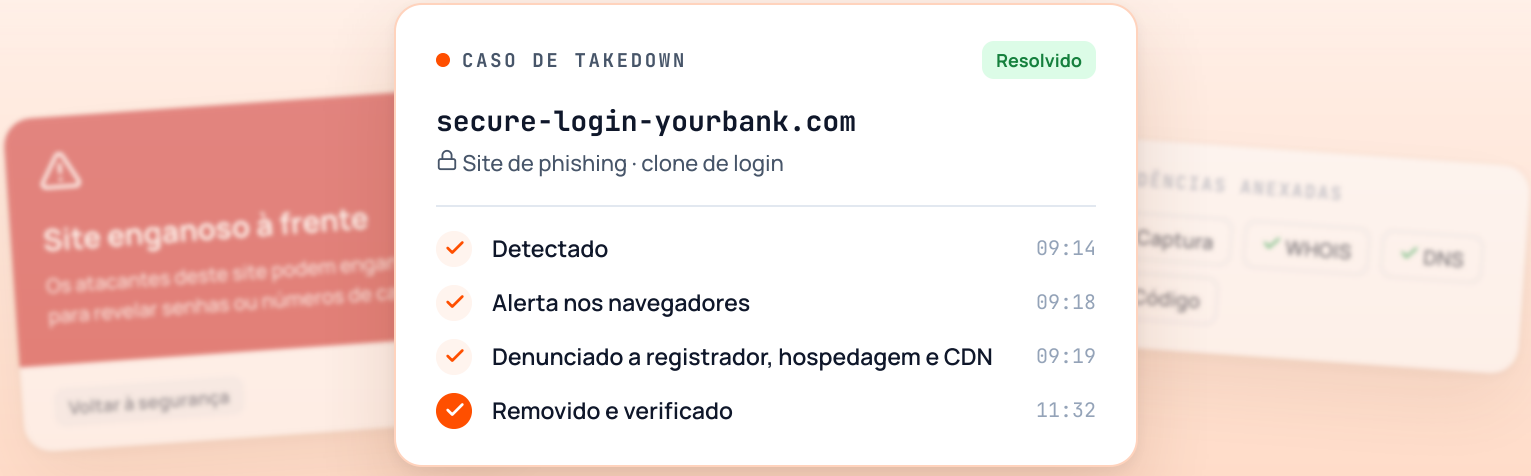
MANUAL DE TAKEDOWN DE PHISHING

Sinalizado em minutos. Fora do ar em dias.

Manual de takedown de phishing.

Os 14 passos, uma denúncia para cada provedor e o que fazer quando ninguém responde.



SUMÁRIO

O que tem aqui

Dez seções, dos primeiros minutos ao relatório final. Leia uma vez para montar o seu processo; durante um incidente, deixe as páginas 4, 8 e 9 à mão.

01 **Por que a velocidade decide** p. 3
Dois relógios: tempo até o alerta e até a remoção.

02 **Os 14 passos** p. 4
Cada passo de um takedown e quais podem ser automatizados.

03 **Confirmar e registrar** p. 5
Tenha certeza de que é phishing e registre antes que mude.

04 **Quem controla o site** p. 6
Registrador, hospedagem, CDN ou plataforma: quem faz o quê.

05 **Primeiro, os navegadores** p. 7
Uma denúncia que protege usuários de Chrome, Safari e Firefox.

06 **Modelos de denúncia** p. 8
Versões para registrador, hospedagem e CDN.

07 **Hospedagens difíceis** p. 10
Cloudflare, Vercel, Netlify e outras plataformas.

08 **Acompanhar e escalar** p. 11
O que fazer quando ninguém responde.

09 **Escolher o caminho** p. 12
Denúncias de abuso, DMCA, URS e UDRP comparados.

10 **Medir** p. 13
Os números que mostram que os sites realmente caíram.

QUATRO FASES, CATORZE PASSOS

01 **Confirmar**
Passos 1–3

02 **Encontrar**
Passos 4–6

03 **Denunciar**
Passos 7–11

04 **Encerrar**
Passos 12–14

PARA QUEM É

Equipes de segurança, SOC e fraude que lidam com sites de phishing que copiam a sua marca, e as agências e MSSPs que fazem isso por elas. Nada aqui exige acesso especial: cada caminho está aberto a qualquer marca com evidências.

SEÇÃO 01

01 Por que a velocidade decide

A maioria dos sites de phishing causa o estrago em horas. Um takedown manual leva dias.

~60%

NO AR MENOS DE 10 MINUTOS

dos domínios de phishing que o Google vê existem por menos de dez minutos. Quando um takedown manual sai, a maioria das campanhas já mudou de lugar.

Fonte: The Hacker News, março de 2024

Dois relógios, não um

Um takedown tem dois objetivos com velocidades diferentes: um alerta no navegador protege a maioria dos visitantes em horas, e a remoção encerra o estrago para todos. Meça separadamente e comece os dois assim que um site for confirmado.

A DISTÂNCIA, EM ESCALA

Escala logarítmica



Fontes: The Hacker News (2024), Cloudflare (2024), The Web Conference (2025), arXiv (2025). Referências completas na página 14.

REGRA PRÁTICA

Nunca faça os passos em sequência

Denuncie ao Google Safe Browsing e a cada provedor no mesmo dia. Esperar a hospedagem antes de contatar o registrador dá tempo ao atacante para mudar a página, e a sua primeira denúncia se perde.

SEÇÃO 02

02 Os 14 passos

Quatro fases. Quase todos os passos são repetitivos, por isso a maioria pode ser automatizada.

01 Confirmar

É phishing, está no ar, que dados coleta?

01 Confirmar que é phishing

Verificar que imita a marca e coleta dados

Quase tudo

02 Registrar evidências

Capturas com data e hora, código da página, a isca

Automatizável

03 Verificar cloaking

Abrir pelo celular, de outros países e navegadores

Automatizável

02 Encontrar

Quem registrou, hospeda e protege o site?

04 Consultar o domínio

RDAP: registrador, contato de abuso, datas, DNS

Automatizável

05 Encontrar a hospedagem

Resolver o IP; buscar o dono e o contato de abuso

Automatizável

06 Olhar atrás do proxy

Se houver um CDN na frente, achar o CDN e a origem

Em parte

03 Denunciar

Todos que podem alertar ou remover, no mesmo dia

07 Navegadores

Google Safe Browsing e Microsoft SmartScreen

Automatizável

08 Registrador

Denúncia de abuso com evidências, pedindo suspensão

Automatizável

09 Hospedagem

As mesmas evidências, pedindo a remoção

Automatizável

10 CDN ou plataforma

O formulário de abuso deles

Automatizável

11 A isca

O e-mail, SMS, anúncio ou rede que a enviou

Em parte

04 Encerrar

Fora do ar em todo lugar, e para sempre

12 Registrar tickets

Cada denúncia, número de ticket e resposta

Automatizável

13 Acompanhar, escalar

Cobrar quem não responde; registro, ICANN ou CERT

Quase tudo

14 Verificar e monitorar

Fora do ar em todo lugar; monitorar o mesmo kit

Automatizável

O QUE AINDA PRECISA DE UMA PESSOA

Casos incomuns (um site legítimo invadido em vez de um falso), escalonamentos que exigem uma notificação jurídica e decidir quando um domínio vale um UDRP.

SEÇÃO 03 · PASSOS 1-3

03 Confirmar e registrar

Antes de denunciar, tenha certeza de que é phishing e registre tudo. Páginas de phishing mudam e somem rápido.

Confirme três coisas

1. **Imita a sua marca:** nome, logo, layout ou textos.
2. **Coleta algo:** uma senha, um número de cartão, um código de uso único. É o sinal mais claro de phishing.
3. **Está no ar agora,** do jeito que seus clientes veriam.

VERIFIQUE O CLOAKING

Mesmo endereço, dois visitantes



Computador Um scanner ou visitante no computador não vê nada.

Celular Uma vítima no celular vê o login clonado.

Muitos kits de phishing mostram a página real só para possíveis vítimas: um celular, um visitante de um país, qualquer um que não seja um scanner conhecido. Registre o que as vítimas veem e diga se ela só aparece para alguns visitantes; senão, quem analisa pode fechar a denúncia.

REGISTRE AS EVIDÊNCIAS

Antes que mude

- A **URL completa** da página, não só o domínio
- O **código da página**, ou um arquivo HAR
- A **sua página real**, para comparar
- **Capturas** com data e hora em UTC
- A **isca**: SMS, e-mail com cabeçalhos, anúncio ou post
- Como as vítimas chegam; quando foi visto

Segurança. Abra páginas suspeitas em um navegador isolado ou máquina virtual, nunca no notebook de trabalho, e nunca digite credenciais reais.

SEÇÃO 04 · PASSOS 4-6

04 Quem controla o site

Um site de phishing costuma envolver três ou quatro empresas, e cada uma pode fazer algo diferente.

ENTRE O SEU CLIENTE E A PÁGINA DE PHISHING

	O QUE PODE FAZER	COMO ENCONTRAR
Navegadores Safe Browsing, SmartScreen	**Alertar** os visitantes enquanto a remoção não sai	Formulários do Google Safe Browsing e do Microsoft SmartScreen
CDN ou proxy ex.: Cloudflare	**Encaminhar** a denúncia à hospedagem e ao dono; às vezes alertar	O IP do site é de um CDN: use o formulário de abuso do CDN
Plataforma Vercel, Netlify, Shopify…	**Remover** o site da plataforma	O endereço está no domínio da plataforma: o formulário de abuso dela
Hospedagem Dona do IP	**Remover** a página e encerrar a conta	O dono do IP no registro regional (ARIN, RIPE, APNIC, LACNIC, AFRINIC)
Registrador Vendeu o domínio	**Suspender** o domínio, para nenhuma página funcionar	O registro RDAP do domínio: “Registrar Abuse Contact Email” (lookup.icann.org)

Se o IP for da Cloudflare ou de um serviço parecido, essa empresa não é a hospedagem: ela encaminha denúncias, então denuncie ao CDN e, se conseguir, direto à hospedagem de origem. Proxies, serviços de privacidade e revendas fazem com que o primeiro contato encontrado muitas vezes não seja o que pode agir.

O WHOIS AGORA É RDAP

Desde 28 de janeiro de 2025, a ICANN não exige mais que os registros de domínios genéricos mantenham o antigo WHOIS; os dados de registro vêm do RDAP. O contato de abuso do registrador continua público, mesmo quando os dados do titular estão ocultos.

2.700+

DOMÍNIOS SUSPENSOS

Desde 5 de abril de 2024, registradores de domínios genéricos devem agir rapidamente diante de evidências concretas de phishing. Nos primeiros seis meses, a ICANN abriu 192 investigações com base nessas regras, que levaram a mais de 2.700 suspensões.

Fonte: ICANN, outubro de 2024

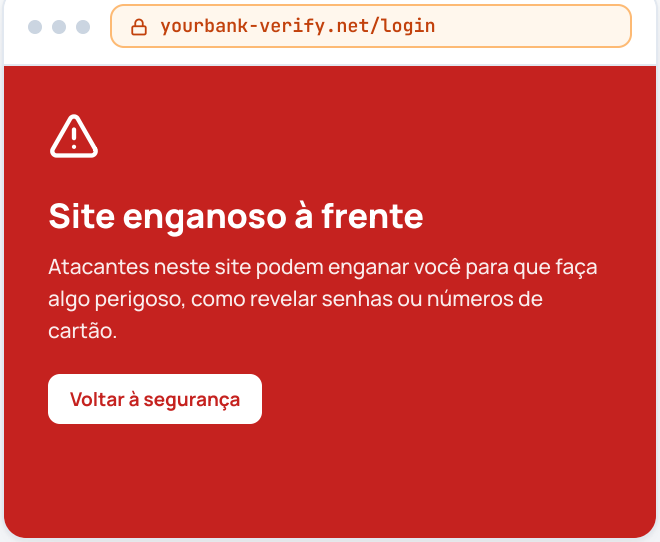
SEÇÃO 05 · PASSO 7

05 Primeiro, os navegadores

Uma denúncia aceita pelo Google Safe Browsing coloca um alerta no Chrome, Safari e Firefox, cerca de 88% dos navegadores em uso.

UMA DENÚNCIA, QUASE TODOS OS NAVEGADORES

Minutos a horas após aceita



NAVEGADORES QUE MOSTRAM O ALERTA



~88% Edge, Opera, outros

Chrome	Google Safe Browsing
Safari	Google Safe Browsing*
Firefox	Google Safe Browsing
Edge	Microsoft SmartScreen
Opera	Listas próprias, ex.: PhishTank

O que faz uma denúncia ser aceita

- **A URL completa da página de phishing,** não o domínio: a página inicial pode parecer inofensiva.
- **Uma página no ar quando o analista olha.** Se só aparece no celular ou em um país, diga.
- **Um formulário que coleta algo:** uma senha, um cartão, um código de uso único.
- **O que ela imita,** com o endereço da sua página real.
- **Uma captura com data e hora,** caso a página mude antes da análise.

⚠ **Um alerta não é um takedown.** O site continua no ar para quem usa um navegador ou app que não consulta a lista, incluindo alguns navegadores dentro de apps. O atacante pode mudar o kit de endereço, e o alerta não acompanha. Denuncie para remoção no mesmo dia. *O Safari usa a Tencent em aparelhos configurados para a China continental; participação segundo a StatCounter.

SEÇÃO 06 · PASSOS 8–10

06 Modelos de denúncia

Envie as mesmas evidências a todos ao mesmo tempo. Os modelos ficam em inglês, a língua das equipes de abuso. Substitua tudo entre ‹colchetes angulares›.

1. Registrador: pedir a suspensão

Nova mensagem · para o contato de abuso do registrador

```
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. **Um assunto que direcione**
   Domínio, marca e a ação pedida, para cair na fila de abuso.
2. **O endereço completo**
   A página que coleta dados, com a hora (UTC) em que foi vista e em que seguia no ar.
3. **Por que é phishing**
   O que copia, o que coleta e como as vítimas chegam.
4. **Evidências**
   As duas capturas, a isca e o código da página.
5. **Um pedido claro**
   Suspensão, citando a política de abuso e as **obrigações sobre abuso de DNS**.

SEÇÃO 06 · CONTINUAÇÃO

2. Hospedagem: pedir a remoção

Nova mensagem · para o contato de abuso da hospedagem

```
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. **Cite a rede**
   Diga que a página está na rede deles, com o IP.
2. **Endereço e servidor**
   A URL completa e o IP do servidor, para acharem a conta.
3. **Remover e guardar logs**
   Remoção, suspensão da conta e logs guardados para as autoridades.

3. CDN ou proxy (por exemplo, Cloudflare)

Use o formulário de abuso do provedor, escolha a categoria de phishing, cole a URL completa e resuma as evidências na descrição. Um CDN normalmente não guarda o site: ele encaminha a denúncia à hospedagem e ao dono, então denuncie também à hospedagem de origem se conseguir identificá-la.

ANTES DE ENVIAR

- ☑ URL completa da página de phishing, verificada de novo
- ☑ Captura com data e hora (UTC), e a nossa página real
- ☑ Que dados coleta e como as vítimas chegam
- ☑ Enviado ao registrador, hospedagem e CDN ao mesmo tempo
- ☑ Denunciado ao Safe Browsing e ao SmartScreen
- ☑ Data de acompanhamento definida

SEÇÃO 07

07 Hospedagens difíceis

Proxies e plataformas serverless mudam a quem você denuncia e o que pede.

PROXY OU HOSPEDAGEM? MUDA O PEDIDO

Um proxy na frente



O proxy não guarda o site. Peça para **encaminhar e alertar**, e denuncie à hospedagem por trás dele.

A plataforma é a hospedagem



A plataforma roda o site. Peça para **remover o deployment** e suspender a conta.

PROVEDOR	PAPEL	O QUE PODE FAZER	SE NADA ACONTECER
Cloudflare (site com proxy)	Proxy	Encaminhar e indicar a hospedagem; mostrar um alerta	Denunciar direto à hospedagem indicada; ao registrador do domínio
Cloudflare Pages / Workers	Hospedagem	Remover o site	Acompanhar na mesma denúncia; Google Safe Browsing
Vercel	Hospedagem	Remover o deployment	Acompanhar; registrador se usa domínio próprio
Netlify, GitHub Pages	Hospedagem	Remover o site ou o repositório	Acompanhar; registrador se usa domínio próprio
Firebase Hosting (web.app)	Hospedagem	Remover o site	Google Safe Browsing

Em um subdomínio de plataforma como **acme-login-secure.vercel.app**, o domínio é da plataforma: nenhum registrador vai suspendê-lo, e pedir isso atrasa a denúncia. Se houver um domínio próprio, denuncie-o ao registrador.

O QUE ESSES PROVEDORES PRECISAM

- **O endereço completo**, com o subdomínio: ele é o site
- **Prova de que está no ar:** capture logo antes de enviar
- **O pedido certo:** remover, encaminhar ou suspender

Enquanto espera. Há relatos públicos de esperas de semanas por denúncias a algumas plataformas. Coloque o endereço no Google Safe Browsing e no SmartScreen no mesmo dia, para os visitantes verem um alerta.

SEÇÃO 08 · PASSOS 11–14

08 Acompanhar e escalar

É aqui que vão a maioria das horas: alguns provedores agem em horas, outros mandam uma resposta automática e nada mais.

Quando ninguém responde

No dia seguinte — **Cobre uma vez**
No mesmo e-mail, se a página continuar no ar, com uma captura nova.

Depois — **Suba um nível**
O registro que administra a extensão (a Verisign para .com) também tem obrigações sobre abuso de DNS.

Sem ação — **Reclame na ICANN**
A equipe de Contractual Compliance aceita reclamações sobre registradores que não agem.

No mesmo dia — **Fontes compartilhadas**
As denúncias ao APWG chegam a muitas empresas de segurança, registradores e hospedagens.

Persistente — **Envolva o seu CERT**
Principalmente quando a hospedagem está em outro país.

O que volta

Respostas de abuso — Abertas 3 · Fechadas

RE	**Re: Phishing on yourbank-verify.net** `abuse@registrar.example` · Your report has been received.	09:21	Automática
PR	**Report forwarded to the host** `noreply@proxy.example` · We are not the hosting provider.	09:24	Encaminhada
HO	**Ticket 77120: phishing content** `abuse@host.example` · We have notified our customer.	Dia 2	Ainda no ar
RE	**Re: [48213] Domain suspended** `abuse@registrar.example` · clientHold applied to the domain.	Dia 3	Suspenso

Ilustrativo. Provedores e domínios fictícios; respostas em inglês, como chegam.

Denuncie também a isca

O site precisa de visitas. Denuncie o canal que as envia: o provedor de e-mail, o remetente do SMS, a plataforma de anúncios ou a rede social que entregou o link. Parar a isca freia a campanha antes mesmo de o site cair.

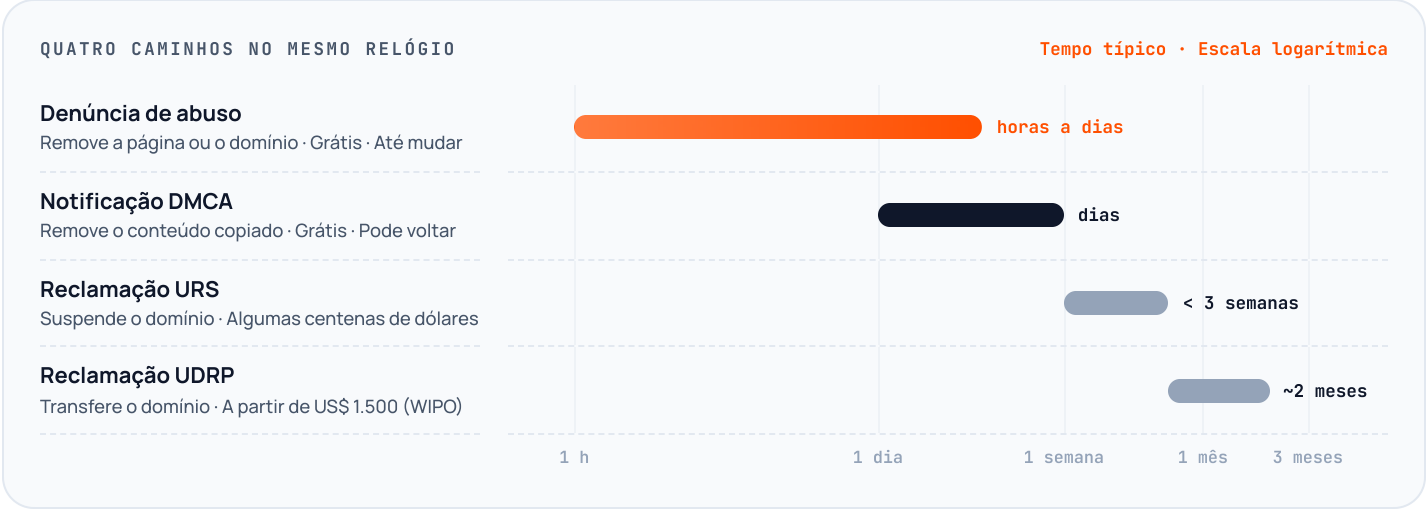
ENCERRE O CASO DIREITO

- ✓ Fora do ar em todo lugar: cada URL, de vários países e dispositivos
- ✓ Monitorando o mesmo kit em novos domínios
- ✓ Evidências e conversas guardadas com o caso
- ✓ Encerrado só quando a remoção é verificada, não quando a denúncia foi enviada

SEÇÃO 09

09 Escolher o caminho

Denúncias de abuso são o caminho mais rápido para um site de phishing no ar. Um UDRP é o único que dá o domínio a você.



Qual caminho para cada situação

SITUAÇÃO	PRIMEIRO	DEPOIS, SE PRECISO
Site de phishing no ar em um domínio imitador	Denúncias à hospedagem e ao registrador; Google Safe Browsing	UDRP se o domínio for reutilizado
Seu site copiado em um domínio sem relação	Denúncia de abuso e notificação DMCA à hospedagem	Monitorar a mesma cópia
Página de phishing em subdomínio de plataforma	O formulário de abuso da plataforma	Nada a disputar
Domínio imitador estacionado, sem conteúdo	Monitorar sinais de ativação	UDRP ou URS se a má-fé for clara
Má-fé clara em um domínio genérico novo	URS para uma suspensão rápida	UDRP para obter o domínio

⚖ **Não é aconselhamento jurídico.** Fale com o seu advogado antes de abrir um UDRP, URS ou DMCA. Use os caminhos em paralelo, nunca em sequência: envie as denúncias de abuso no mesmo dia e abra um UDRP junto só se quiser o domínio.

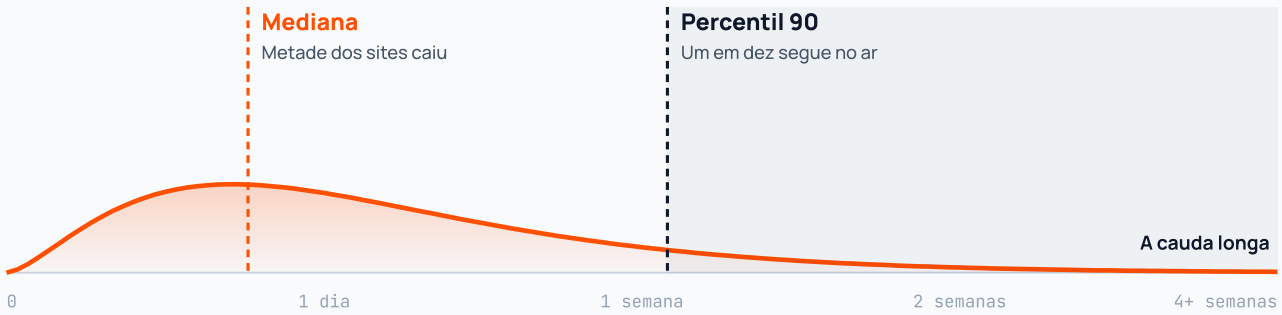
SEÇÃO 10

10 Medir

Meça ameaças removidas, não denúncias enviadas. Médias escondem sites no ar por semanas.

TEMPO ATÉ A REMOÇÃO EM UM TRIMESTRE

Formato ilustrativo



MÉTRICA	COMO MEDIR	POR QUE IMPORTA
Tempo até o alerta	Confirmação → alerta; mediana e percentil 90	A rapidez com que a maioria fica protegida
Tempo até a remoção	Confirmação → fora do ar; mediana e percentil 90	O número que encerra o estrago
Taxa de resolução	Casos fora do ar e verificados, não “denunciados”	Um caso parado continua coletando dados
Taxa de reincidência	O mesmo kit ou operador em um novo domínio	Campanhas ou sites isolados?
Horas de trabalho	Tempo de analista por takedown, por fase	O custo de fazer à mão

O que não conta

- ✕ **Denúncias enviadas** ou **takedowns solicitados:** uma denúncia não é uma remoção.
- ✕ **Alertas:** encontrar um site não protege ninguém até ele ser sinalizado e removido.
- ✕ **Uma média sozinha:** um em cada dez sites no ar por semanas pode parecer bom na média.

DEFINA UMA LINHA DE BASE

Meça os seus próximos dez takedowns

Registre os dois relógios e as horas de trabalho de cada um. Isso mostra para onde vai o tempo e o que vale automatizar primeiro.

COMO A SENTRIKE FAZ ISSO

O manual, executado por agentes de IA

A Sentrike executa cada passo do takedown. A sua equipe acompanha cada caso sem precisar fazer o trabalho.

01 **Detectado**
Novos domínios, certificados e páginas, 24 horas por dia

02 **Verificado**
Pacote de evidências: capturas, WHOIS, DNS, código

03 **Alertado**
Denunciado ao Google Safe Browsing

04 **Denunciado**
Denúncias de abuso à hospedagem e ao registrador

05 **Removido**
Acompanhado até a remoção ser verificada

Os agentes de IA da Sentrike confirmam que o site é malicioso, montam o pacote de evidências, denunciam ao Google Safe Browsing para que Chrome, Safari e Firefox alertem os visitantes em minutos, enviam denúncias de abuso à hospedagem e ao registrador e acompanham até o site sair do ar e a remoção ser verificada. A maioria dos sites é encontrada antes que clientes os denunciem.

Pare de correr atrás de takedowns.

Veja os sites de phishing que usam a sua marca hoje, e a rapidez com que caem.

Solicitar acesso →

sentrike.ai/pt/takedown

FONTES

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