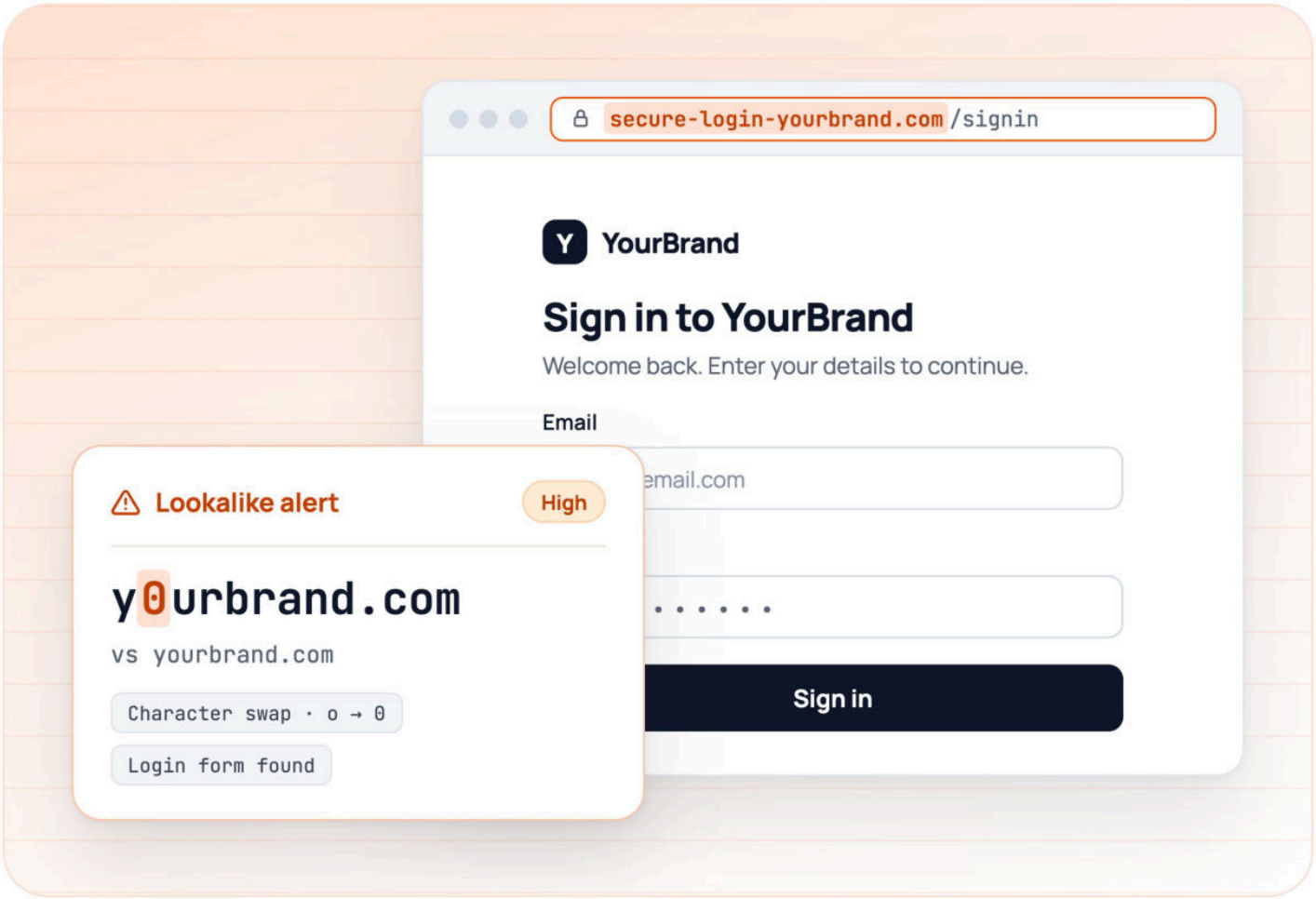
Sentrike

FIELD GUIDE
Brand impersonation · 2026

SPOT IT EARLY

Top 10 Signs Attackers Are Impersonating Your Brand

Your customers can't tell the difference. Here's how you can.



WHY THIS MATTERS NOW

Impersonation used to look fake. Not anymore.

AI lets attackers clone your site, your logo, and your tone of voice in minutes. The old tells, like typos, blurry logos, and clumsy layouts, are gone.

The victim is your customer. The damage lands on you: on your brand's reputation, on your support team's queue, and on your fraud losses.

77%

of security leaders say cyber-enabled fraud and phishing increased in the past year.

Source: World Economic Forum, Global Cybersecurity Outlook 2026.

THE 10 SIGNS

One sign per page

01 Lookalike Domains Near Your Name

02 Cloned Login Pages

03 "Your" Emails You Never Sent

04 Fake Support Accounts on Social

05 Text Messages Using Your Name

06 Fake Payment and Billing Pages

07 Counterfeit Storefronts and Offers

08 Your Assets Loading on Strange Domains

09 Fraud Spikes Without a Breach

10 Reported Sites That Stay Online

Keep this guide handy for anyone who owns your brand, your login page, or your customer inbox.

01 Lookalike Domains Near Your Name

Attackers register domains that are one glance away from yours.

Expect typosquats (yourbrnd.com), character swaps (y0urbrand.com), add-on words (yourbrand-login.com, secure-yourbrand.net), and new TLDs (yourbrand.co). Many sit dormant until a campaign launches.

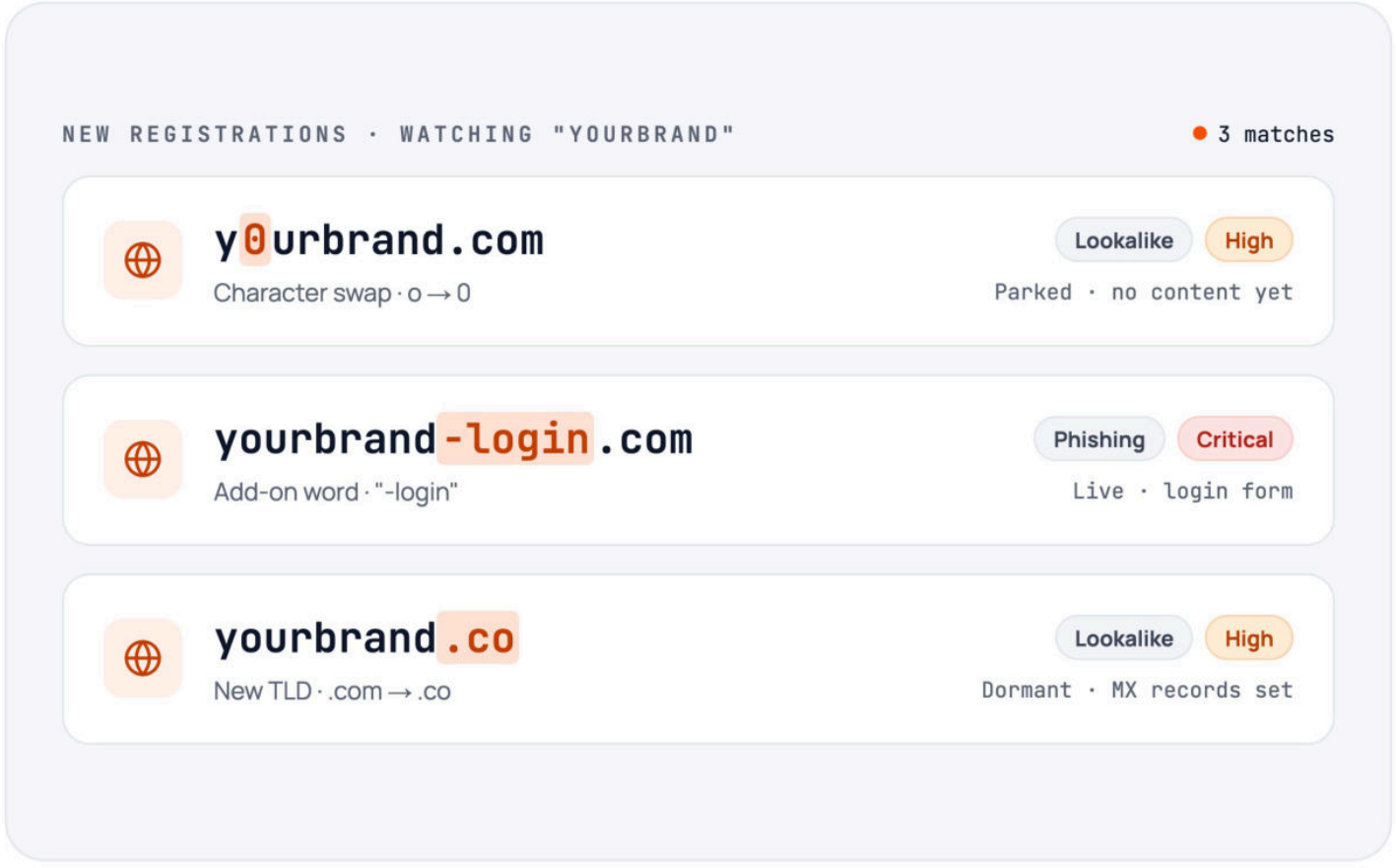
WHAT TO CHECK

Watch new registrations containing your brand name, not just exact matches. The registration is the earliest warning you'll get.

~20 days

Maliciously registered brand-impersonating domains stayed online about 20 days on average after detection.

Source: "Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks," arXiv, 2025.



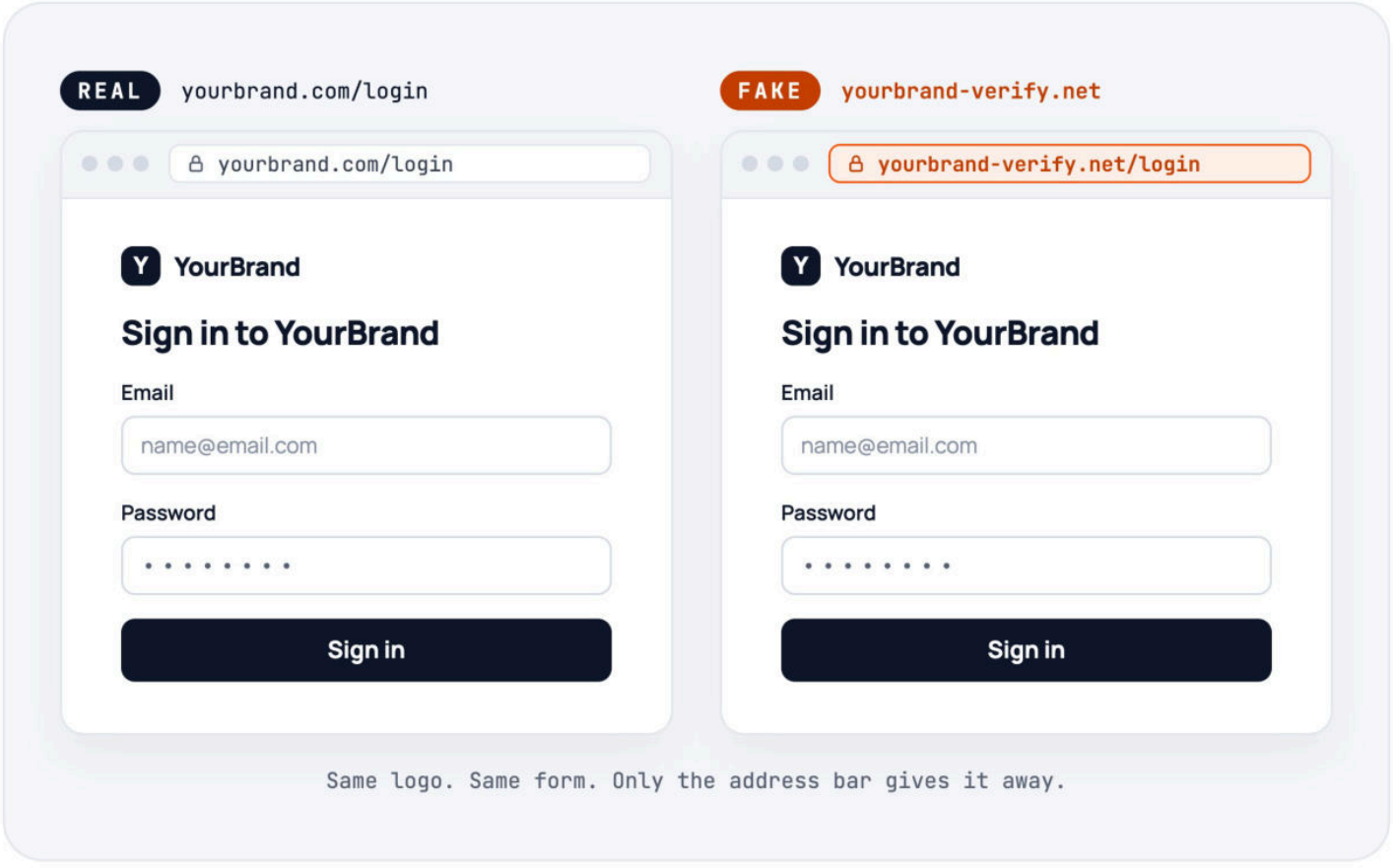
02 Cloned Login Pages

A fake login page doesn't look fake anymore.

Your logo, colors, and form fields can be copied pixel-for-pixel. Some clones proxy the real site in real time, so they capture MFA codes too.

WHAT TO CHECK

The domain is the only thing attackers can't fake. Teach customers your one official login URL, and monitor for pages that copy your login form.



Same logo. Same form. Only the address bar gives it away.

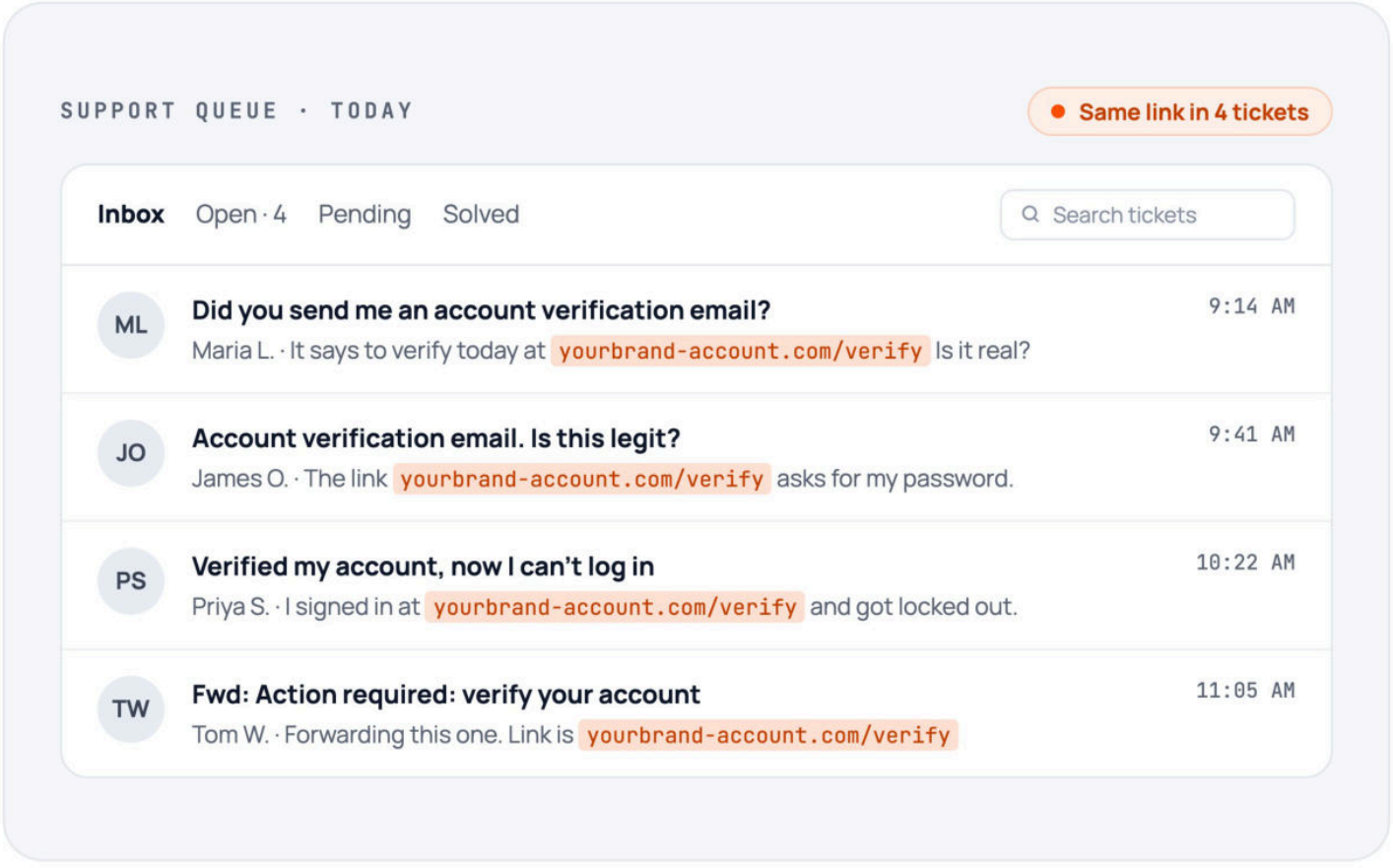
03 "Your" Emails You Never Sent

Your support queue sees impersonation before your security team does.

Customers ask about a "security alert," "refund," or "account update" you never sent. Individually, these tickets look like noise. Together, they're a campaign.

WHAT TO CHECK

Give support a one-click way to forward suspicious links to security. Three similar tickets in a day is an incident.



04 Fake Support Accounts on Social

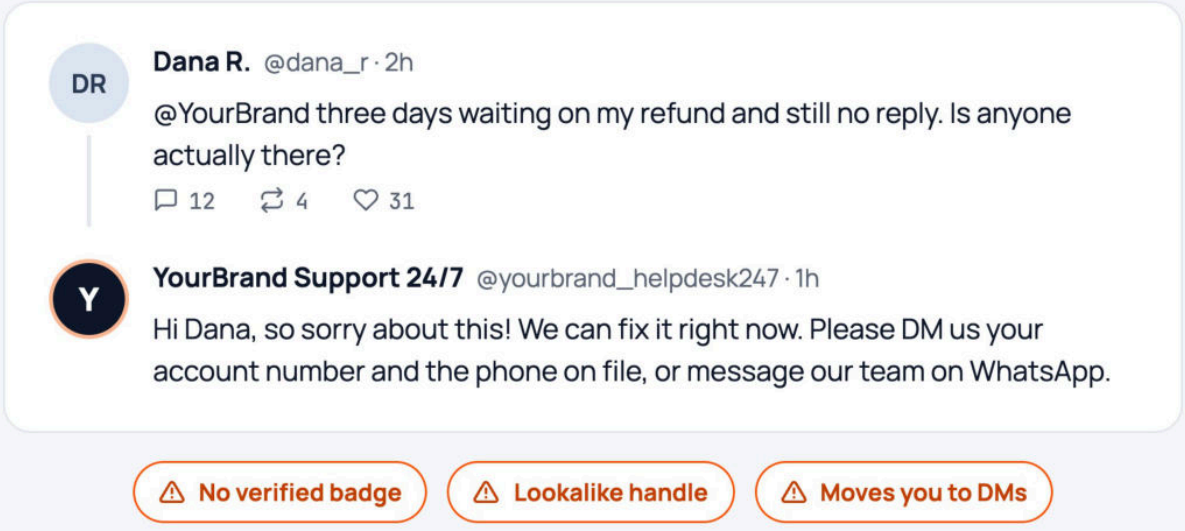
Impersonation is often the opening move of a scam.

Fake "YourBrand Support" profiles reply to real customer complaints, then move the conversation to DMs, WhatsApp, or a "verification" link.

WHAT TO CHECK

Search your brand name plus "support" or "help" across platforms weekly, and list your official handles on your website.

43.8% **of social-media threats in Q1 2026 were impersonation.**
Source: APWG Phishing Activity Trends Report, Q1 2026.



05 Text Messages Using Your Name

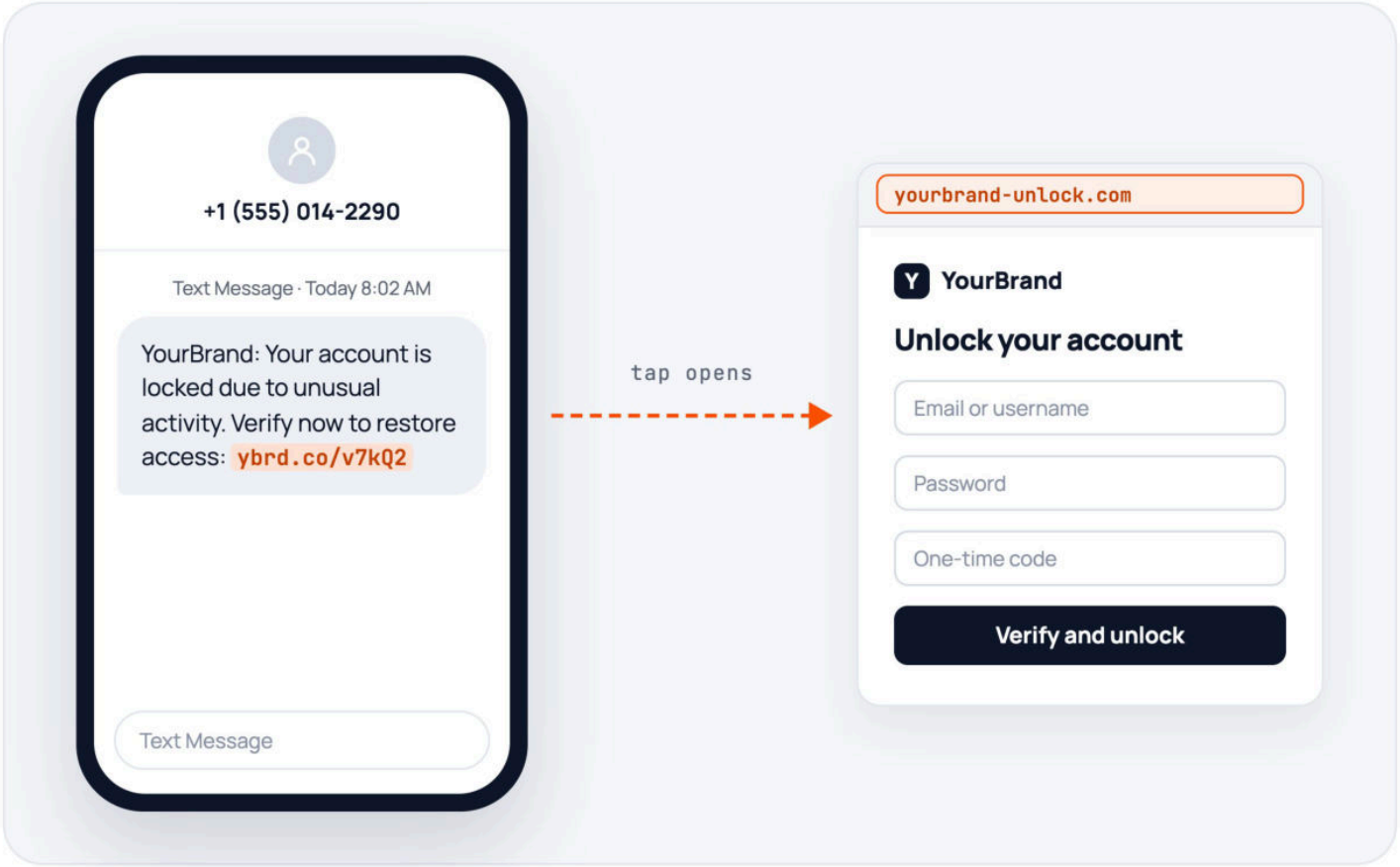
The lure moved to the phone, where links are hardest to inspect.

"Your YourBrand account is locked. Verify now:" plus a short link. On mobile, customers can't hover to see where a link really goes.

WHAT TO CHECK

State publicly what you will never ask for by SMS, and monitor for the landing pages these texts point to.

+40% **Smishing rose 40% from Q1 to Q2 2026.**
Source: APWG Phishing Activity Trends Report, Q2 2026.



06 Fake Payment and Billing Pages

"Payment failed" is one of the oldest lures, and still one of the best.

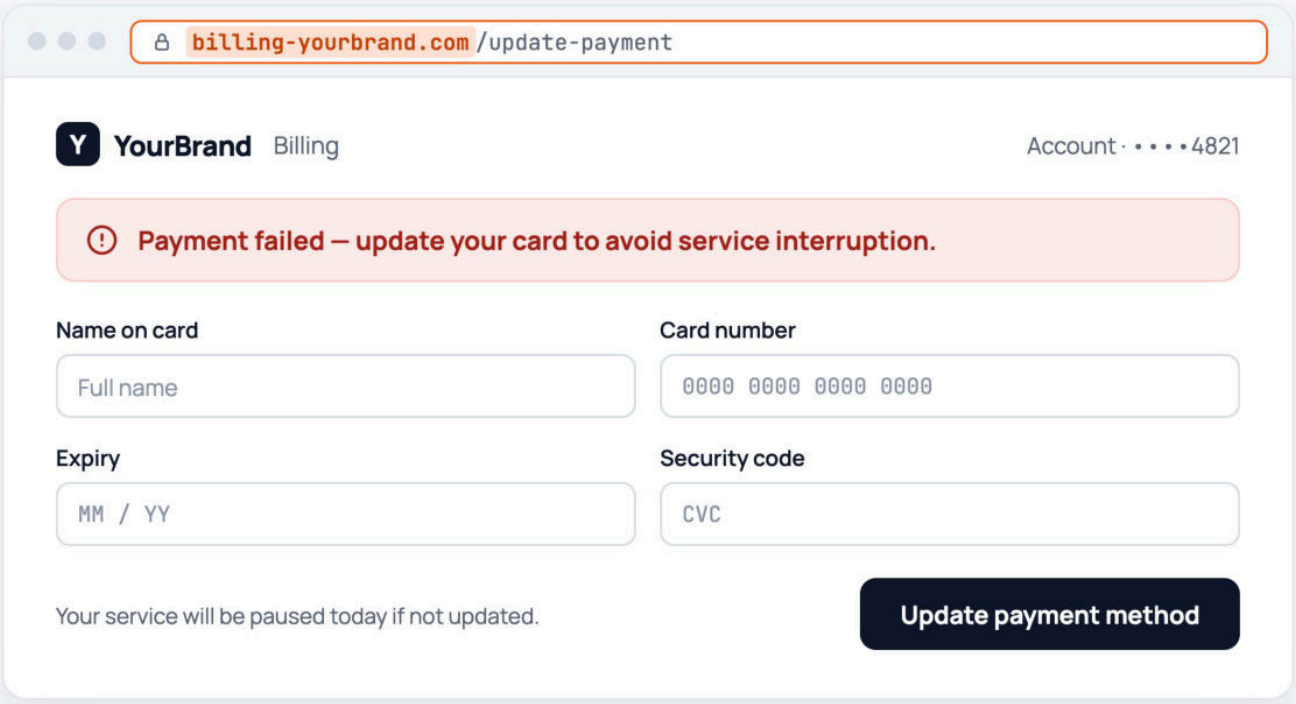
Fake invoices, failed-payment notices, and "update your card" pages harvest card data under your brand. Customers pay attention because money is involved.

WHAT TO CHECK

Any page outside your domain asking for card or bank details in your name is a takedown candidate, not a curiosity.

37% of respondents said they or someone in their network was hit by invoice or payment fraud in the past year.

Source: World Economic Forum, Global Cybersecurity Outlook 2026.



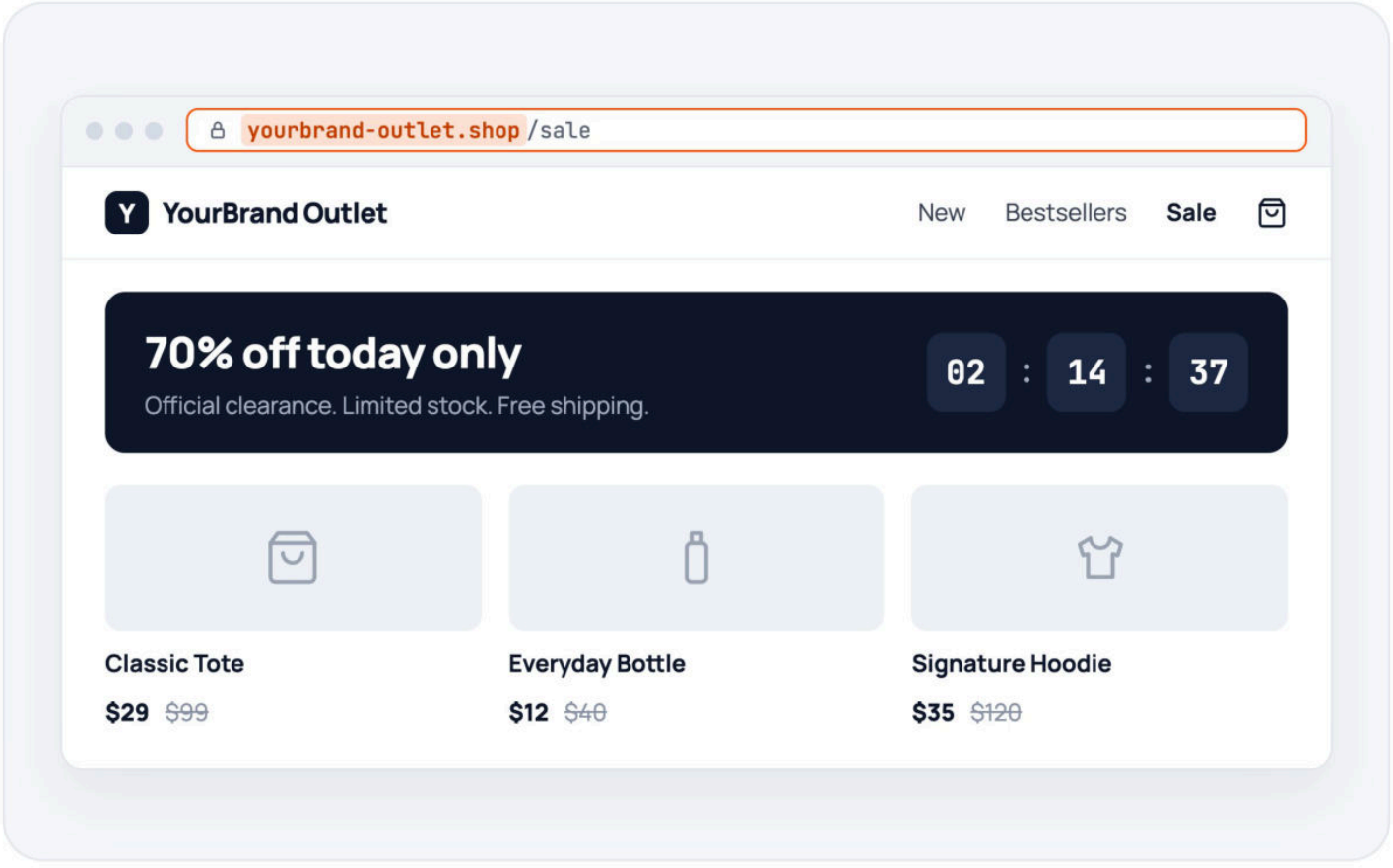
07 Counterfeit Storefronts and Offers

Too-good-to-be-true discounts, wearing your logo.

Replica shops and "exclusive offer" pages use your product images to take payments and deliver nothing. Customers don't blame the scammer. They blame you.

WHAT TO CHECK

Watch for your product names and imagery on domains you don't own, especially around launches and sale seasons.



08 Your Assets Loading on Strange Domains

Clones often borrow your real logo and files.

Lazy clones hotlink your images, fonts, or scripts straight from your servers. Your web logs and CDN referrers can reveal pages you've never seen.

WHAT TO CHECK

Review referrers to your logo and login assets for unknown domains. Each one is a lead.

CDN REFERRER REPORT · LAST 7 DAYS

● 2 unknown referrers

REFERRER	ASSET	HITS	STATUS
yourbrand.com	/assets/logo.svg	48,210	Owned
app.yourbrand.com	/login/app.css	31,904	Owned
yourbrand-secure.net	/assets/logo.svg	1,204	Unknown
help.yourbrand.com	/assets/logo.svg	9,876	Owned
account-yourbrand.co	/login/app.css	386	Unknown
partners.yourbrand.com	/fonts/brand.woff2	2,117	Owned

09 Fraud Spikes Without a Breach

When nothing was hacked but accounts are still being taken over.

A sudden rise in password resets, failed logins, or new payees is often the downstream effect of a phishing site collecting your customers' credentials.

WHAT TO CHECK

When fraud or account-takeover (ATO) metrics jump, look outward for an active phishing site before looking inward.

32% of respondents said they or someone in their network experienced identity theft in the past year.

Source: World Economic Forum, Global Cybersecurity Outlook 2026.



10 Reported Sites That Stay Online

Finding the fake site is half the job. Removing it is the other half.

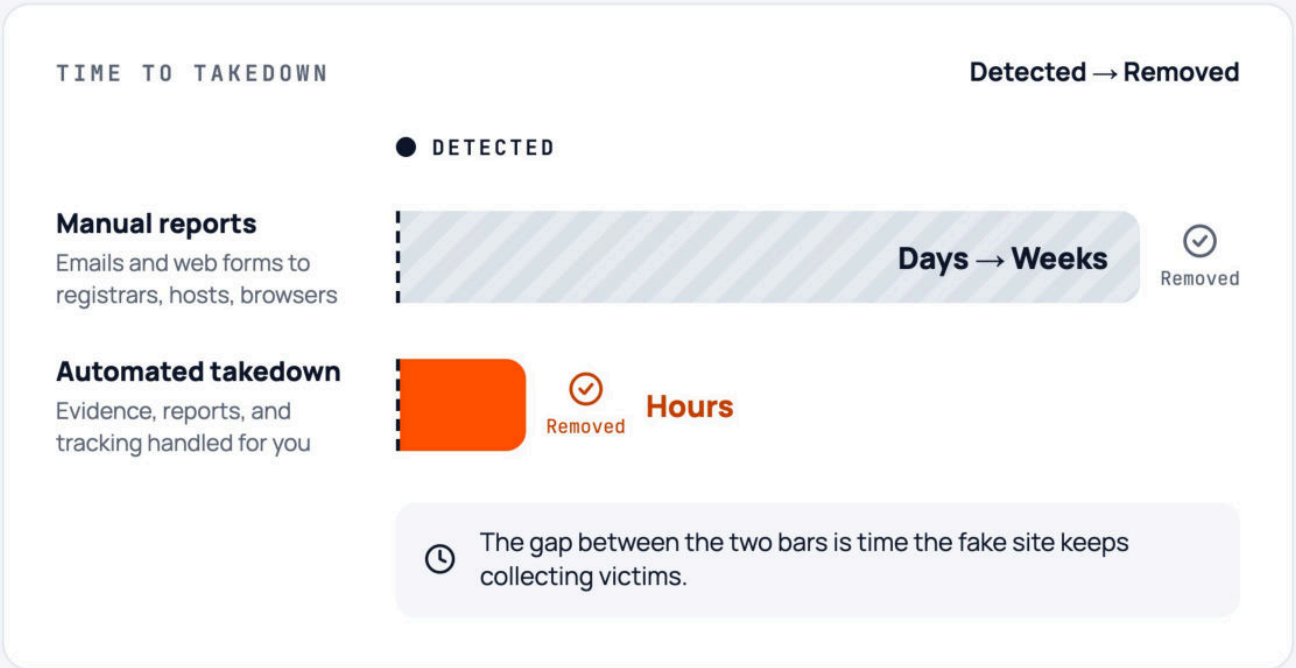
Manual abuse reports to registrars and hosts can take days or weeks. In that window, browsers don't automatically block most phishing sites.

WHAT TO CHECK

Measure time to takedown, not just time to detection. Every hour a fake site is live, it keeps collecting victims.

~18% **In one study, Google Safe Browsing detected only about 18% of phishing sites, taking about 4.5 days on average.**

Source: Lim et al., "7 Days Later: Analyzing Phishing-Site Lifespan After Detected," WWW 2025.



WHAT TO DO NEXT

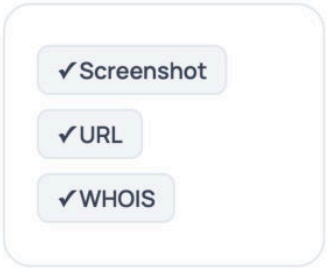
What to do when you spot one.

Four steps, in order. Speed matters more than perfection.

00 CAPTURE

Capture evidence

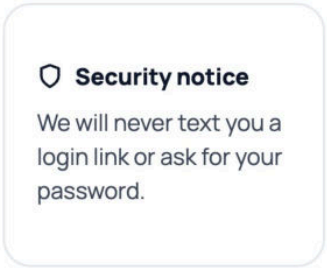
Screenshot, URL, and WHOIS, before the page changes.



01 WARN

Warn customers

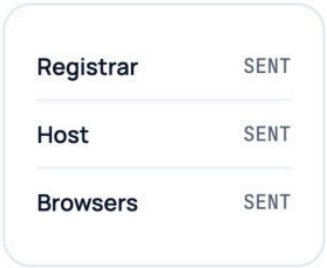
Through official channels only: your site, app, and verified accounts.



02 REPORT

Report it

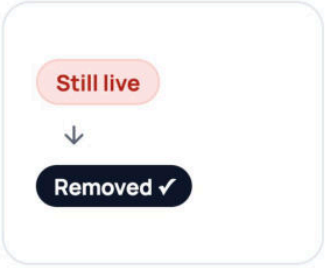
To the registrar, the host, and browser safety programs.



03 TRACK

Track it

Until it's actually gone, not just reported.



Doing this manually for every lookalike doesn't scale. That's the gap Sentrike closes.

24/7 monitoring

Domains, sites, and social profiles, watched around the clock.

Detection in minutes

Evidence is collected automatically with every alert.

One-click takedown

Tracked until the impersonating site is removed.

AI-POWERED BRAND PROTECTION

Find fake sites before your customers do.

Sentrike monitors your brand 24/7 and takes down impersonators autonomously.

Request access →

Schedule a call →

sentrike.ai/early-access

Sentrike

AI-powered brand protection and takedowns

SOURCES

77% · 37% · 32%	World Economic Forum, Global Cybersecurity Outlook 2026.
~20 days	"Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks," arXiv, 2025.
43.8%	APWG Phishing Activity Trends Report, Q1 2026.
40%	APWG Phishing Activity Trends Report, Q2 2026.
18% · 4.5 days	Lim et al., "7 Days Later: Analyzing Phishing-Site Lifespan After Detected," WWW 2025.

© 2026 Sentrike · sentrike.ai

Brands shown in examples are fictional.