



PUBLIC

THREAT INTELLIGENCE SNAPSHOT · HEALTHCARE & LIFE SCIENCES

Healthcare & Life Sciences Threats

Most confirmed impersonation of healthcare brands runs through paid advertising, almost all of it on one platform. Lookalike websites carry under a tenth of it.

VERTICAL

Healthcare & Life Sciences

REPORTING WINDOW

01JUN2026 to 30SEP2026

ISSUED

14OCT2026

PREPARED BY

DJ Peterson
Doppel SECR

01 EXECUTIVE SUMMARY

Between 77% and 90% of confirmed impersonation against healthcare brands runs through paid advertising. The lookalike websites most monitoring programs are built around account for under 11% of it. Facebook advertising carried 99.8% of the paid-ad activity, and Facebook carried 90.3% of confirmed social impersonation.

Activity on this surface rose sharply through September, in the run-up to the Medicare open enrollment period that opens on 15OCT2026 and closes on 07DEC2026. The brands drawing the most activity are health plans and Medicare products, which is the pattern that enrollment-season fraud produces.

A second and separate threat runs against staff. Voice phishing against IT help desks, aimed at password resets and multi-factor re-enrollment, is the vector sector bodies have flagged repeatedly since 2024, and it is supported by registered domains built to look like corporate sign-on portals. Domains therefore carry a small share of the patient-facing volume and a meaningful share of the staff-facing risk. A low share of activity is not a reason to retire domain monitoring, and it is a reason to stop treating domain volume as the measure of the whole problem.

Posture for the sector: ad-led against patients, identity-led against staff, and seasonally timed. Individual brands will sit at different points on this curve. Health plans and Medicare products carry the heaviest advertising exposure, while provider systems carry more of the help-desk and sign-on risk, so the sector mix is the baseline to measure a program against, not a forecast for any one brand.

SURFACE EXPOSURE

ELEVATED**Most confirmed activity runs on advertising platforms, which domain monitoring does not cover**

Programs built on domain registration and certificate transparency see about a tenth of confirmed impersonation items in this sector at most. The domain surface still matters for the staff-targeted sign-on lookalikes that sector bodies name as the primary vector against healthcare staff, so coverage is best measured by surface rather than by domain volume.

PAID ADS

77-90% Of confirmed activity, every month

FACEBOOK ADS

99.8% Of confirmed paid-ad abuse

DOMAINS

Under 11% Of confirmed activity

SIGN-ON LOOKALIKES

76 domains Registered against healthcare brands

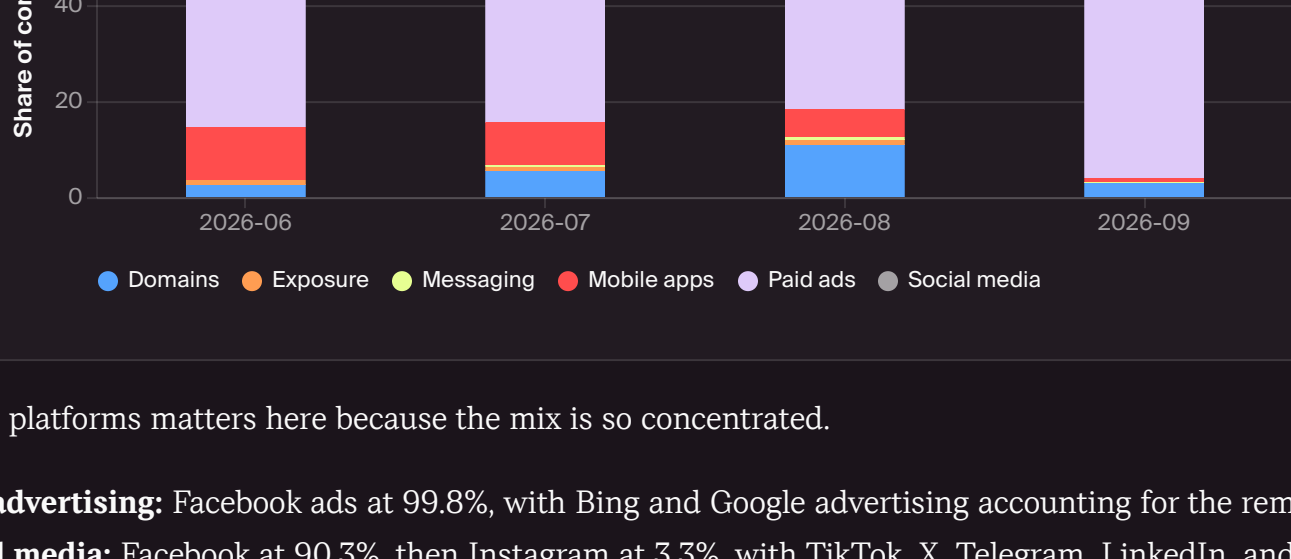
02 WHERE CONFIRMED ACTIVITY CONCENTRATES

Paid advertising led every month of the window, moving from 84% of confirmed activity in June to 90% in September. Second place rotated among mobile applications, lookalike domains, and social media, and none of them held it for more than two months. Lookalike domains never exceeded 11%, and in two of the four months sat below 3%.

The practical reading is that a large share of impersonation against healthcare brands is being monetized through advertising inventory, which costs an actor less setup than a hosted phishing site. An actor who buys an ad inherits the platform's targeting, its reach, and a measure of implied legitimacy, without registering a domain, standing up hosting, or obtaining a certificate. Nothing in a certificate-transparency feed or a registrar watchlist fires on that route.

The September rise is consistent with the calendar. The [Medicare open enrollment period](#) opens on 15OCT2026 and closes on 07DEC2026, and the brands drawing the most activity in this window are health plans and Medicare products. The [Senior Medicare Patrol](#) warned on 28SEP2026 that health insurance scams pick up during open enrollment and that scammers pay to appear at the top of search results, which is the same advertising route Doppel's confirmed activity follows. Doppel's activity in the same months of the prior year moved in the same direction. Treat the enrollment period as the point of maximum exposure and staff for it.

CONFIRMED ACTIVITY BY SURFACE, SHARE PER MONTH



Naming the platforms matters here because the mix is so concentrated.

- **Paid advertising:** Facebook ads at 99.8%, with Bing and Google advertising accounting for the remainder.
- **Social media:** Facebook at 90.3%, then Instagram at 3.3%, with TikTok, X, Telegram, LinkedIn, and WhatsApp in the low single digits.
- **Messaging:** telecommunications channels, meaning SMS, at 93.3%.

Exposure, meaning leaked credentials and related data, is tracked as its own surface and is not counted in the impersonation figures above.

03 WHAT A DOMAINS-ONLY VIEW MISSES

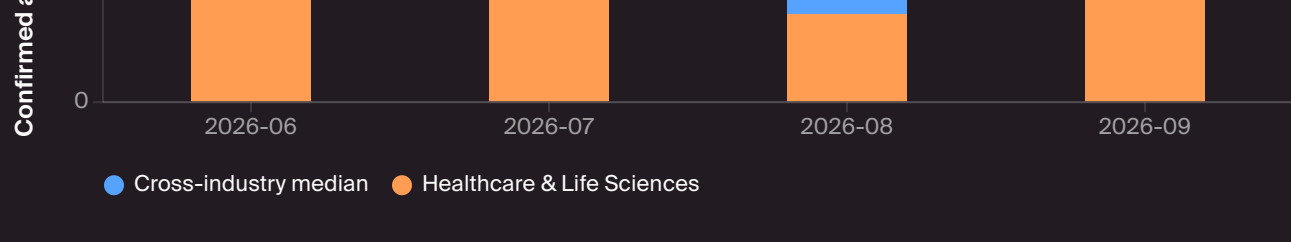
ACROSS DOPPEL TELEMETRY, 74.5% OF CAMPAIGNS NEVER TOUCH A DOMAIN SURFACE

Of the campaigns that do involve a domain, 61.3% also run on at least one other surface, so catching the domain addresses only part of the operation.

The pattern holds across every sector in Doppel telemetry, and the healthcare channel mix is an unusually sharp instance of it: a monitoring program built on domain registration and certificate transparency would miss most of what is confirmed against healthcare brands. Public fraud reporting points the same way. In [FTC Consumer Sentinel data for 2025](#), social media, phone, email, and text together accounted for more than half of fraud reports with a reported loss, none of which a domain watchlist sees.

04 MARKET COMPARISON

CONFIRMED ACTIVITY PER BRAND AGAINST THE CROSS-INDUSTRY MEDIAN



Healthcare brands drew about a fifth less confirmed activity per brand than the cross-industry median by the end of the window.

Lower relative volume is not lower risk. Healthcare brands carry patient data, prescription fulfilment, benefits enrollment, and claims processing, so a single successful impersonation reaches further than its volume suggests. Benefits and prescription lures convert directly, which raises the consequence of each successful attempt. Program sizing should follow the surface mix and per-incident consequence rather than the sector's position on a cross-industry median.

05 SIGN-ON PORTALS AND THE HELP DESK

The activity above targets patients. A separate line of attack targets staff, and it is the one sector bodies have warned about most consistently since 2024.

[Health-ISAC's advisory of 24JUL2026](#), the [incident report it circulated through the American Hospital Association on 24AUG2026](#), and a [2024 joint advisory from CISA, the FBI, and HHS](#) describe the same chain. An attacker calls the IT help desk posing as a clinician or executive locked out of a clinical system, uses urgency that a care setting makes credible, and asks for a password reset, a multi-factor change, or enrollment of a new device. Generative voice tools make the impersonation harder to refuse. Where the call succeeds, the payoff is the organization's single sign-on tenant and the cloud platforms behind it. Health-ISAC reported an observed increase in successful attacks on health sector organizations by this route, and the August incident report described a typosquatted sign-on portal hosted behind a content delivery network as the supporting infrastructure. Health-ISAC also published a [Doppel-authored playbook](#) on conversational social engineering in care settings in August 2026, covering the same chain and the help-desk controls that counter it.

SIGN-ON PORTAL LOOKALIKES ARE BEING REGISTERED AGAINST HEALTHCARE BRANDS

Across the reporting window, Doppel indexed 76 distinct registered domains carrying sign-on and identity-provider tokens in their hostnames. The registration pattern is systematic rather than opportunistic: families of near-miss spellings of one health-plan brand, each published under a sign-on style hostname.

Whether a lookalike sign-on domain is serving a login page or sitting dormant when first indexed, registration precedes use, and the domain is the component a visiting call needs in place before the call is made. Health-ISAC's August incident report recommends tracking exactly these registrations.

VERIFICATION AT THE HELP DESK IS THE CONTROL THAT BREAKS THE CHAIN

The call is the entry point, and the durable access comes from the identity change that follows it.

- **Impact:** A single successful reset or multi-factor re-enrollment converts a phone call into access to the sign-on tenant and the clinical and business platforms behind it.
- **Do:** Require out-of-band callback to a number held on record before any password reset, multi-factor change, or new-device enrollment, add a second approver for privileged accounts, and rehearse the refusal with voice-based exercises rather than email-only phishing tests.

06 KEY FINDINGS AND PRIORITY ACTIONS

Healthcare has been among the most breached sectors in the United States for over a decade, and the [HHS Office for Civil Rights breach portal](#) remains the authoritative public record of its scale. [FTC Consumer Sentinel data](#) show that scams starting on social media produced 2.1 billion dollars in reported losses in 2025, more than any other contact method, with Facebook ahead of every other platform and paid advertising among the tools scammers use to reach targets. Doppel's healthcare telemetry shows the same shape: Facebook first, with advertising as the carrier.

PAID ADVERTISING IS THE PRIMARY IMPERSONATION SURFACE

Between 77% and 90% of confirmed activity ran through paid ads in every month of the window.

- **Impact:** A brand-protection program scoped to domains and search engines will not see most confirmed impersonation of its brand.
- **Do:** Treat advertising platforms as in-scope at the program level, and give fraud and communications teams a single intake path for ad-based impersonation reported by patients or staff.

META PROPERTIES CARRY ALMOST THE ENTIRE CONFIRMED PICTURE

Facebook advertising accounted for 99.8% of confirmed paid-ad abuse, and Facebook accounted for 90.3% of confirmed social impersonation.

- **Impact:** Platform relationships and escalation paths concentrated on a single provider become the determining factor in response speed.
- **Do:** Establish and periodically test a named escalation contact and a documented reporting path with Meta before it is needed under pressure.

DOMAIN VOLUME IS A POOR MEASURE OF PROGRAM HEALTH

Lookalike domains never exceeded 11% of confirmed activity, and across Doppel telemetry 74.5% of campaigns never touch a domain surface. The domains that do appear in this sector include a systematic set of staff-targeted sign-on lookalikes.

- **Impact:** A program judged by how many lookalike domains it catches will report health while the advertising surface carrying most activity goes unmeasured.
- **Do:** Track brand-protection coverage by surface, and read domain findings for what they indicate about staff-targeted credential attacks alongside their raw count.

SMS CARRIES 93% OF CONFIRMED MESSAGING ACTIVITY

Telecommunications channels made up 93.3% of confirmed messaging activity in the vertical.

- **Impact:** Benefits, prescription, and appointment lures delivered by SMS reach patients outside any channel the organization controls.
- **Do:** Publish and repeat a clear statement of which communications the organization will and will not send by text, and give patients one verifiable number to check against.

BELOW-MARKET VOLUME IS NOT BELOW-MARKET RISK

Healthcare brands ended the window about a fifth below the cross-industry median for confirmed activity per brand.

- **Impact:** Benchmarking against other sectors can justify underinvestment in a sector where each incident carries regulatory and patient-safety consequences.
- **Do:** Size the program against per-incident consequence and the regulatory environment it operates under.

Findings are based on Doppel telemetry across a global customer base, with strongest coverage in North America. Impersonation figures reflect analyst-confirmed activity.



Our mission is to protect the world from social engineering attacks every day. Our AI-native defense anticipates deception and eliminates threats.

1B+ INDICATORS ANALYZED DAILY

300+ TRUSTED CUSTOMERS

doppel.com

Prepared by Doppel SECR - Social Engineering Counterintelligence & Research

© Doppel Inc. 2026. All Rights Reserved.