Doppel

OUTPACING WHAT'S NEXT
IN SOCIAL ENGINEERING

2026 SOCIAL ENGINEERING PREDICTIONS

Defending Digital Trust

AI-Driven Deception & How Organizations Need to Respond

DOPPEL.COM

©2026 DOPPEL INC.

Foreword

The cybersecurity industry has spent the past 20 years investing far more in protecting infrastructure than in protecting people. While protecting infrastructure is foundational to any security program, treating social engineering as inevitable rather than a reducible risk reflects a limited approach.

In 2026, relying on that perception is dangerous.

The adversarial landscape has shifted dramatically. We haven't left the era of hacking infrastructure; exploiting zero-day vulnerabilities in code still happens, but we have entered a new era of hacking cognition.

This shift is quantifiable: 60% of all data breaches involve the human element, creating a massive vulnerability that legacy infrastructure alone can't patch.[1]

With the commoditization of generative AI, attackers have industrialized the art of social engineering. They no longer need to break down your firewall; they simply need to synthesize the voice of your CFO, the face of your recruiter, or the login page of your payroll provider with pixel-perfect accuracy.

The predictions contained in this report are born from Doppel's analysis of millions of attacks and a full variety of threat vectors. They paint a picture of a world where 'seeing is believing' is a liability. A world where the attack surface is no longer just your servers or networks, but your people's trust.

Legacy defenses, often point solutions that protect a single channel and rely on static blocklists, aren't equipped to protect businesses, employees, or consumers from today's modern threats. They can't stop an attack that begins on LinkedIn, pivots to a deepfake video call, and ends with compromised credentials on a mirrored domain.

Modern attacks require modern defense. The future of defense is multi-channel, multi-layered, and AI-native. It's about fighting the new AI threats with new AI defenses.

Welcome to the age of AI-native deception.

Kevin Tian

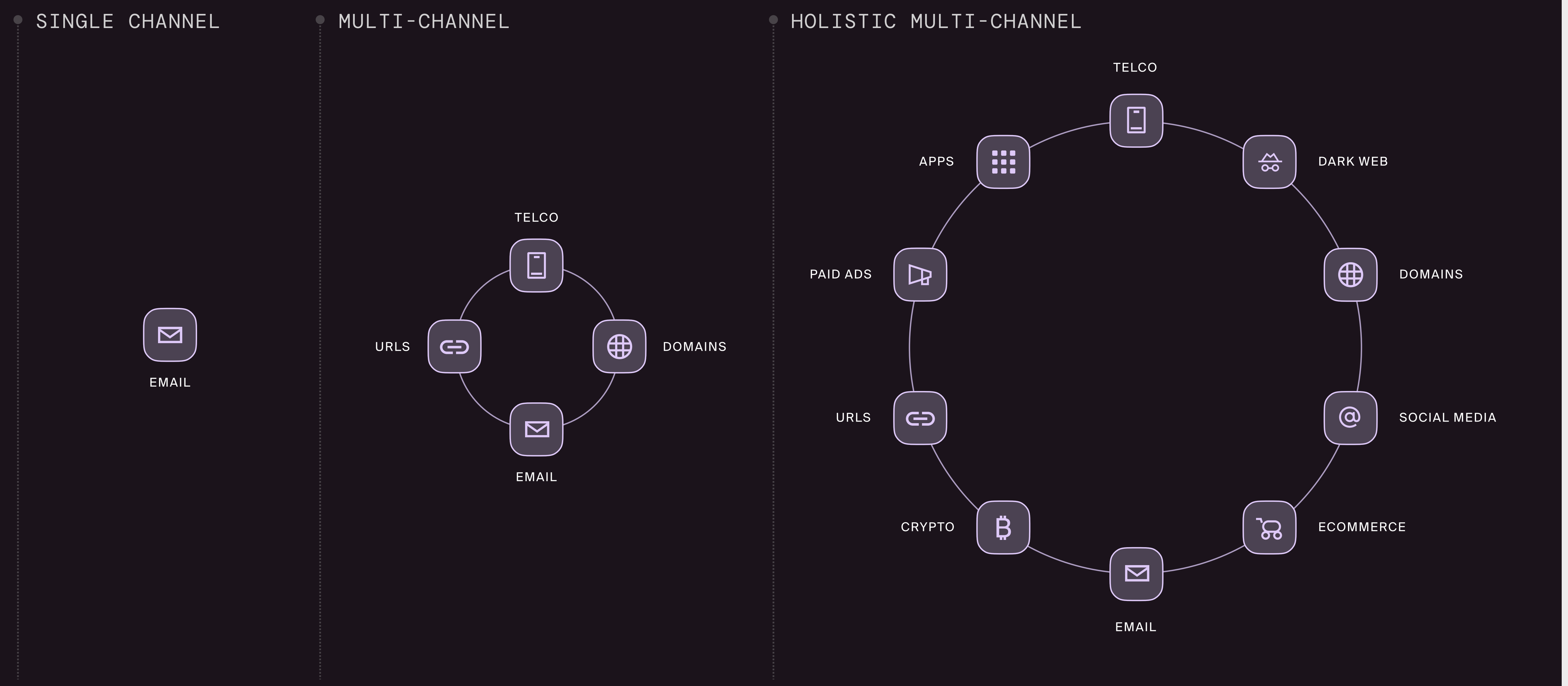
Kevin Tian
Co-Founder & Chief Executive Officer, Doppel

Executive summary

Social engineering is the dominant operating model of modern cybercrime.

> Throughout 2026, the distinguishing line between legitimate communication and malicious attacks is vanishing.

This report outlines four critical shifts that will define the threat landscape of 2026. Driven by Doppel's internal threat intelligence and analysis of cross-channel attack vectors, we find that the convergence of multi-channel distribution and agentic AI is creating a "perfect storm" for enterprise security teams.



THE EXPANSION OF THREATS

KEY PREDICTIONS

The Reality Gap

Synthetic media will render traditional verification methods obsolete.

We predict that by the end of 2026, it'll be effectively impossible for the human eye or ear to distinguish between legitimate media and malicious deepfakes without technological assistance.

The Multi-Channel Siege

Attackers are moving laterally across platforms.

Doppel's data reveals that over 44% of all campaigns are now multi-channel, coordinating attacks across domains, social media, SMS, voice, video, and paid advertising to encircle victims.

The Velocity War

Manual takedowns stand no chance against AI.

With attackers spinning up infrastructure in seconds, the only defense is an AI-native offense. Doppel has tracked a 5x speedup in resolution times using AI automation, bringing mitigation down to 12 hours compared to the industry standard of days or weeks.

The Code Word Society

As impersonation scales, corporate and personal verification will regress to analog methods.

Safe words and pre-shared secrets will become the standard operating procedure for authorizing transactions and sensitive data transfers.

The end of 'seeing is believing'

DEEPFAKES & THE EROSION OF MEDIA INTEGRITY

Photographic and video evidence have been the gold standard of truth for a century. If you saw a video of your CEO announcing a merger, it was happening. If you saw a news anchor reporting a crisis, it was real.

In 2026, that assumption will be challenged.

The scale of this shift is already becoming apparent, with research indicating that deepfake attempts occur every 5 minutes.[2]

> By the end of 2026, it'll be nearly impossible to distinguish legitimate media from malicious deepfakes created to deceive.

While 2024 and 2025 saw the early adopters of this technology — primarily in election interference and public figure impersonation — 2026 will mark the year this technology becomes a standard attack vector.

This threat is being accelerated by the very tools designed to help us. We're currently seeing a rise in companies producing 'benevolent' deepfakes and synthetic video avatars made to create content more easily and enhance productivity.

These tools allow executives to 'attend' multiple town halls simultaneously or enable customer support agents to appear as localized, friendly avatars.

Attackers are parasitic; they'll weaponize this familiarity. Employees lack the instinct to question everyday interactions and media, such as a call from a colleague or a video of an executive, because they're trusting a familiar voice or visual.

Reputational Fragility

Public figures and brands will be vulnerable to synthetic media attacks that look and sound real, deployed through seemingly innocuous social interactions.

A fake video of a CEO making a racist remark or announcing a stock sell-off can wipe billions off a market cap in minutes, before the truth can be established.

Verification Crisis

Organizations will be forced to establish entirely new verification systems.

The question will no longer be "Is this video real?" but "Can this media be cryptographically proven to originate from a trusted source?"

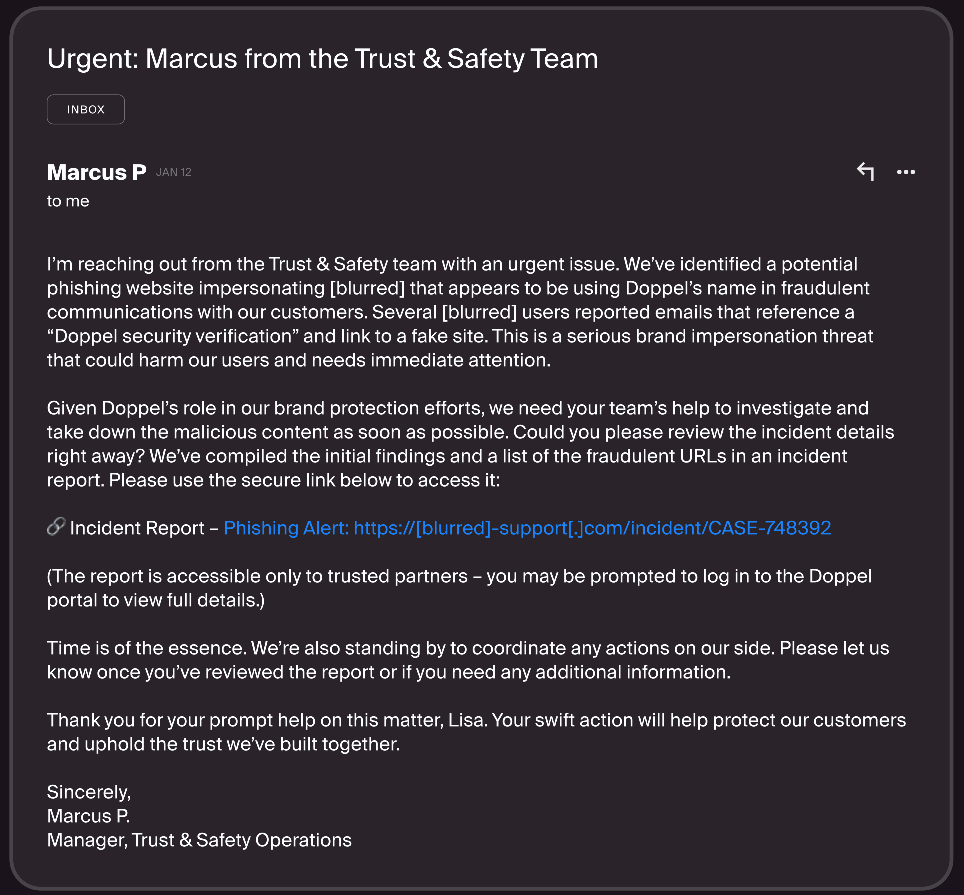
THE END OF ‘SEEING IS BELIEVING’

Attackers weaponize familiarity

The timeline of increasingly sophisticated identity compromise

ERA 1

Poorly Written Email



Urgent: Marcus from the Trust & Safety Team

INBOX

Marcus P JAN 12

to me

I’m reaching out from the Trust & Safety team with an urgent issue. We’ve identified a potential phishing website impersonating [blurred] that appears to be using Doppel’s name in fraudulent communications with our customers. Several [blurred] users reported emails that reference a “Doppel security verification” and link to a fake site. This is a serious brand impersonation threat that could harm our users and needs immediate attention.

Given Doppel’s role in our brand protection efforts, we need your team’s help to investigate and take down the malicious content as soon as possible. Could you please review the incident details right away? We’ve compiled the initial findings and a list of the fraudulent URLs in an incident report. Please use the secure link below to access it:

🔗 Incident Report – Phishing Alert: https://[blurred]-support[.]com/incident/CASE-748392

(The report is accessible only to trusted partners – you may be prompted to log in to the Doppel portal to view full details.)

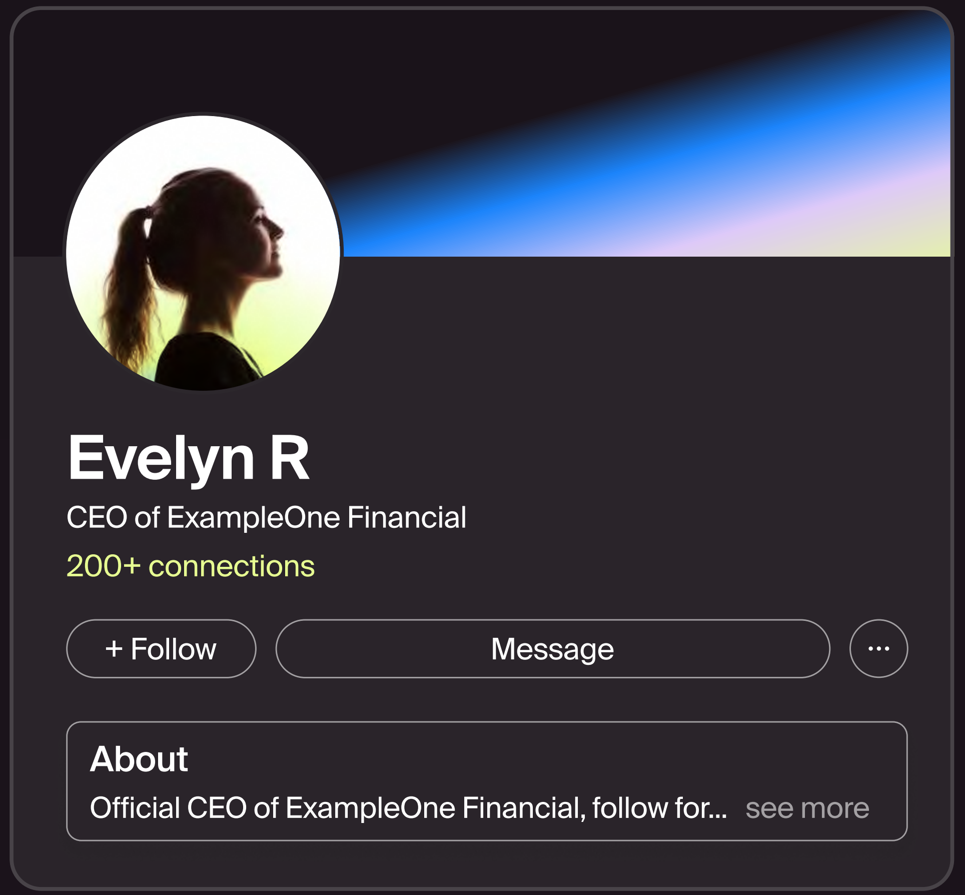
Time is of the essence. We’re also standing by to coordinate any actions on our side. Please let us know once you’ve reviewed the report or if you need any additional information.

Thank you for your prompt help on this matter, Lisa. Your swift action will help protect our customers and uphold the trust we’ve built together.

Sincerely,
Marcus P.
Manager, Trust & Safety Operations

ERA 2

Spoofed Display Name & Static Profile Photo



Evelyn R

CEO of ExampleOne Financial

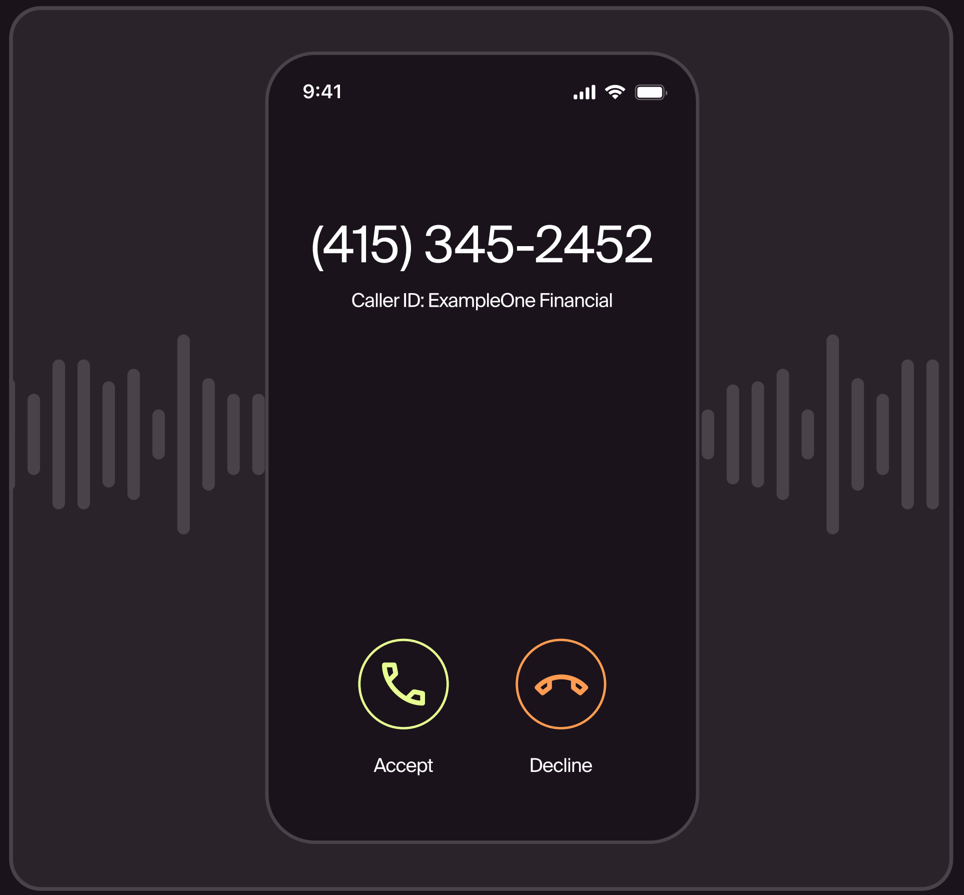
200+ connections

About

Official CEO of ExampleOne Financial, follow for... see more

ERA 3

Audio-Only Deepfake

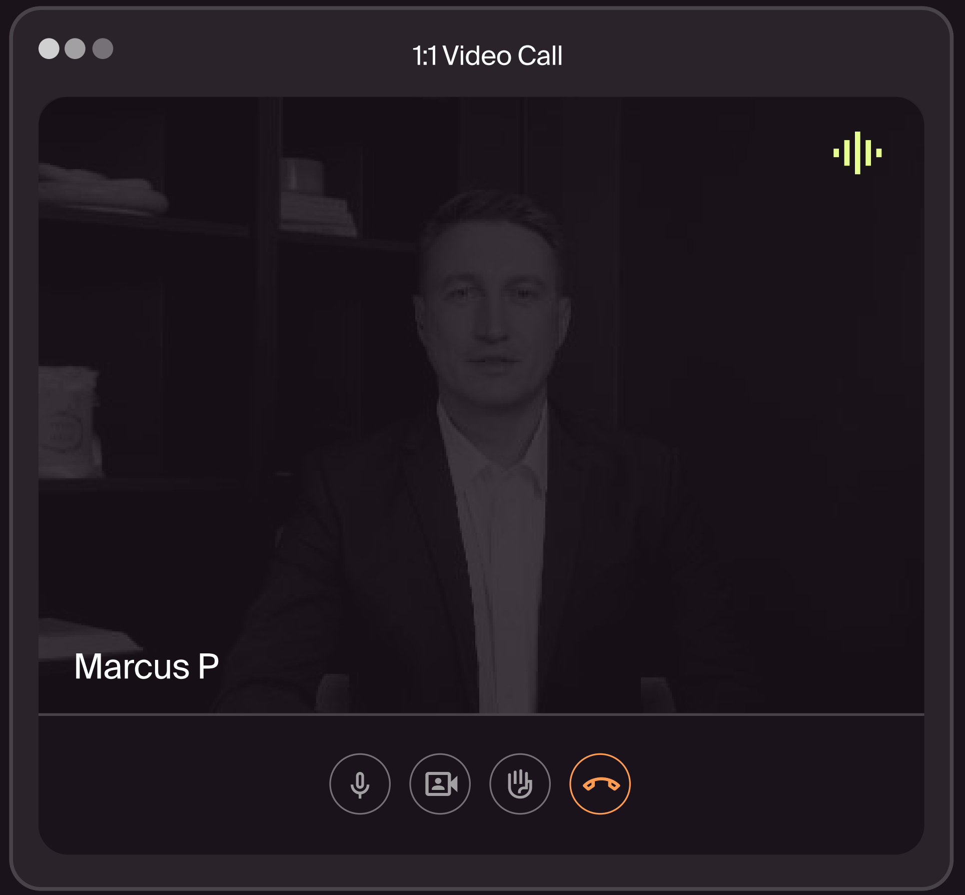


(415) 345-2452

Caller ID: ExampleOne Financial

ERA 4

Real-Time, Interactive Video & Audio Clone with Perfect Lip-Sync



“

Early in my career, security awareness was all about training employees not to click on bad links. That approach worked when the threats were simple and the attacks were obvious. But today, the challenge goes far beyond human judgment; cybercriminals are using AI to create convincing impersonations and build attacks that even the most well-trained employee can fall for. We can’t rely on awareness alone anymore; we need technologies that protect people proactively, stopping these threats before they ever reach their inbox.

Bobby Ford
Chief Strategy and Experience Officer, Doppel

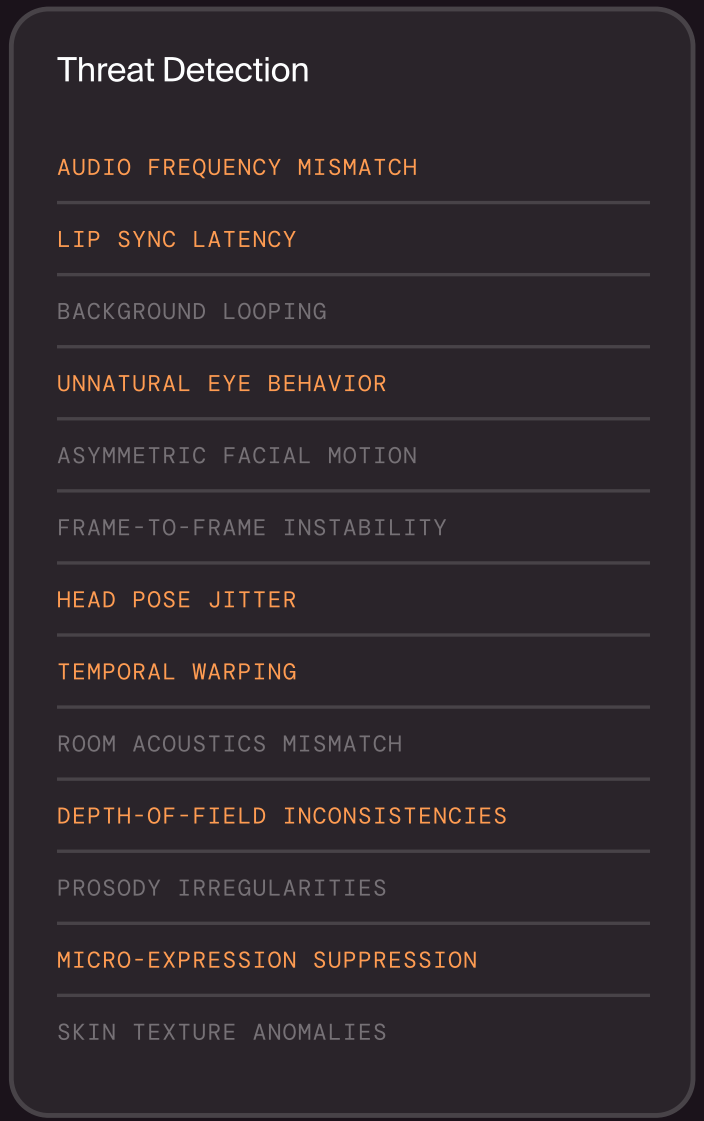
The Trojan Horse of productivity

VIDEO CALLS BECOME AN ATTACK VECTOR

Remote work normalized the video call. It's the primary venue for high-stakes decision-making.

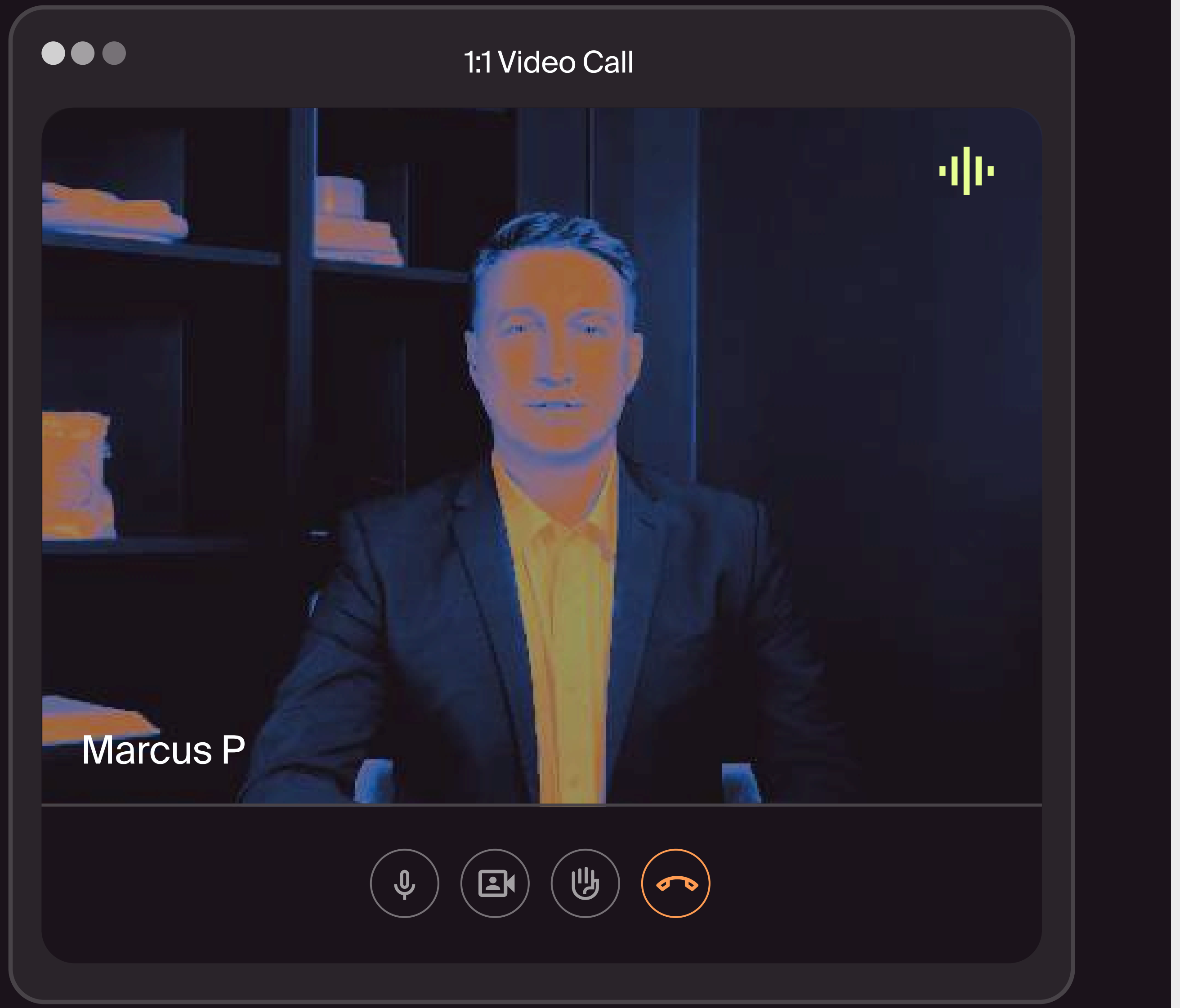
Because it feels live and personal, we lower our guard. We assume that the person on the screen, whose background is the familiar office we've seen often, is actually them.

> In 2026, the tools we use to connect will become the weapons used to compromise us. We predict a surge in real-time video injection attacks.



Threat Detection

- AUDIO FREQUENCY MISMATCH
- LIP SYNC LATENCY
- BACKGROUND LOOPING
- UNNATURAL EYE BEHAVIOR
- ASYMMETRIC FACIAL MOTION
- FRAME-TO-FRAME INSTABILITY
- HEAD POSE JITTER
- TEMPORAL WARPING
- ROOM ACOUSTICS MISMATCH
- DEPTH-OF-FIELD INCONSISTENCIES
- PROSODY IRREGULARITIES
- MICRO-EXPRESSION SUPPRESSION
- SKIN TEXTURE ANOMALIES



Infiltration

An attacker compromises a lower-level vendor email account, perhaps that of a scheduler or an executive assistant at a known supplier.

Setup

They schedule a legitimate Zoom or Teams meeting with a target executive at a financial institution.

Switch

Using real-time AI face-swapping and voice cloning (trained on public YouTube interviews of the person they are mimicking), the attacker joins the call.

Extraction

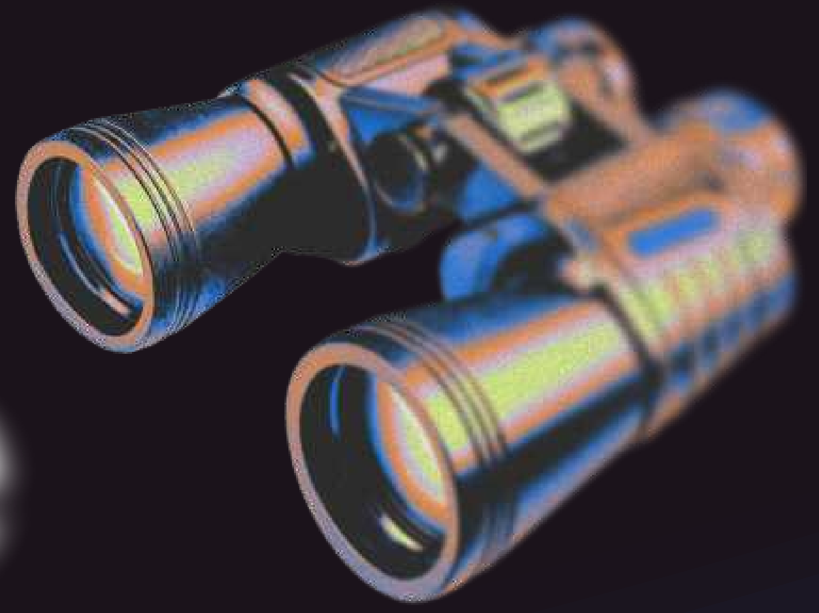
They don't ask for a wire transfer immediately (that triggers alarms). They ask for access. "I'm locked out of the admin portal. Can you screen share and show me the config?"

This vector bypasses traditional endpoint security entirely.
It targets the human instinct to trust visual cues.

Doppel's threat intelligence indicates that as text-based models become easier to detect, adversaries are pivoting to high-bandwidth formats (video/audio) where detection tools are less mature.

Defending against this requires a Zero Trust communication culture. It necessitates the ability to detect artifacts in video streams — such as unnatural blinking patterns and audio-visual desynchronization — in real time, something the human eye cannot consistently do.

Tips for Spotting a Deepfake



Study the Face & Eyes

They don't ask for a wire transfer immediately (that triggers alarms). They ask for *access*. "I'm locked out of the admin portal. Can you screen share and show me the config?"

Check Lip-Sync & Audio

Watch the mouth closely:
Do lip shapes match sounds, or do words seem slightly out of sync with lip movement?

Look at Lighting, Shadows, and Background

See if lighting on the face matches the background; inconsistent shadows or highlights are major clues.

Watch Body Movement & Expressions

Notice whether the head and body move together naturally; jerky turns, a stiff body with only the face moving, or limbs that distort when moving can indicate manipulation.

Verify Outside Video

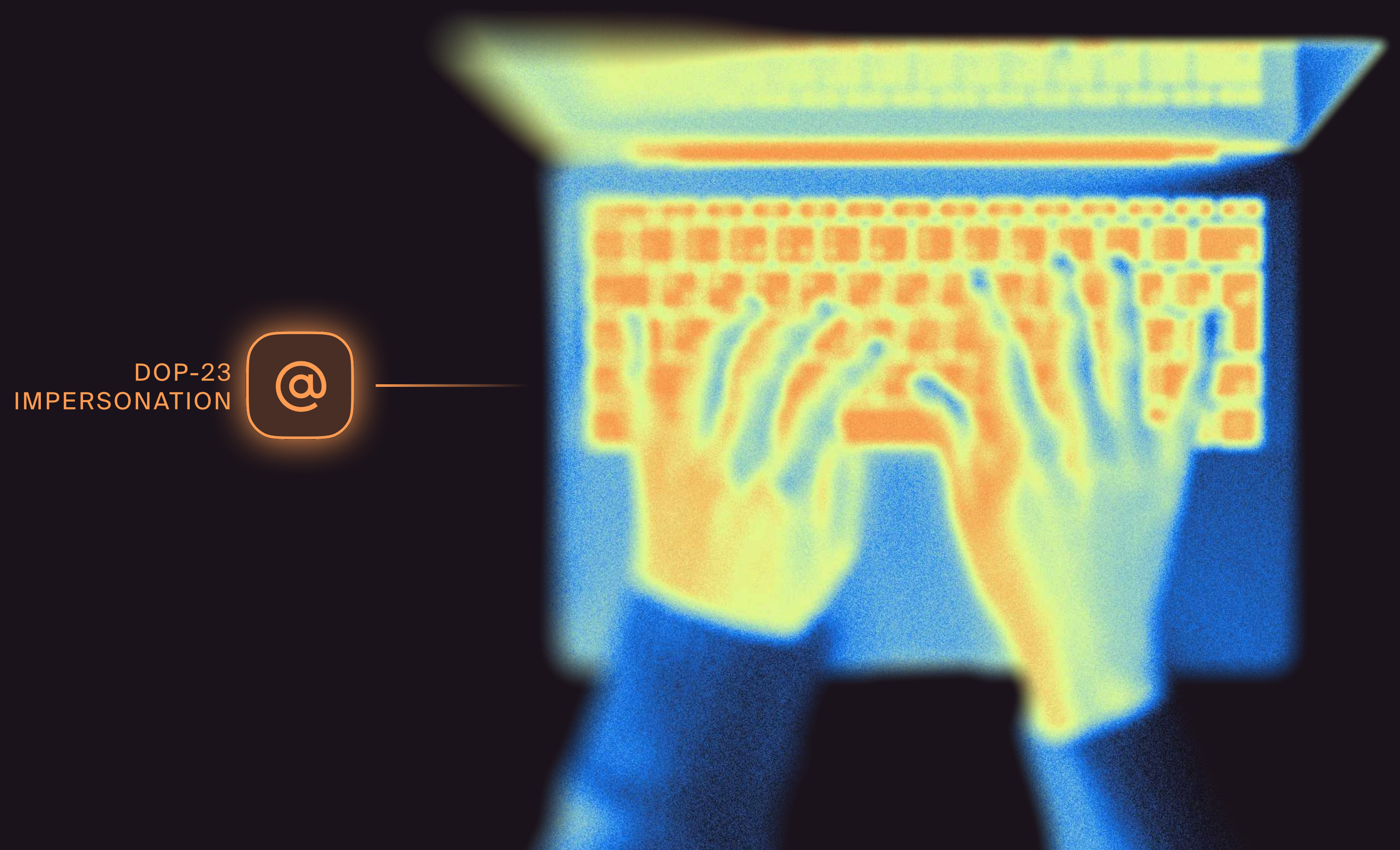
Look for an additional source:
If it's a video call, try communicating with the real individual through another channel, such as email or phone. If it's a video, check with other sources to see if they report the same clip.

The industrialization of human trust

RECRUITMENT SCAMS

The labor market creates a massive emotional vulnerability. People seeking jobs are eager, compliant, and willing to share personal data. In the wake of the economic shifts of 2025, a large pool of job seekers has created a target-rich environment.

2026 will see a spike in fake recruiters on platforms like LinkedIn. These aren't simple data scraping operations; they're deepfake-enabled messages and interviews designed to steal identities and trick candidates into installing malware under the guise of 'coding tests' or 'knowledge assessments.'



BY THE NUMBERS

84 MILLION	220 MILLION	<10 SECONDS
The number of fake accounts LinkedIn reportedly stopped or restricted in the first half of 2025 alone.[3]	Reported losses to job scams in the first half of 2024.[4]	The amount of audio required to produce a convincing AI voice clone.[5]

The rise in these attacks is forcing a cultural shift that bleeds from the enterprise into the home.

When a frantic call comes in from a 'loved one' or a 'boss' claiming an emergency, emotional cues like tone and urgency — once the markers of truth — are now the weapons of the attacker.

We predict that by 2026, families and corporate teams will adopt 'challenge-response' authentication protocols.

Scenario	A Chief Financial Officer calls an employee on the finance team, demanding an urgent transfer.
Defense	The employee asks for the safe word.
Result	If the caller fumbles, hangs up, or tries to bypass the request, the attack is neutralized.

Trust will evolve from something we feel to something we must actively confirm.

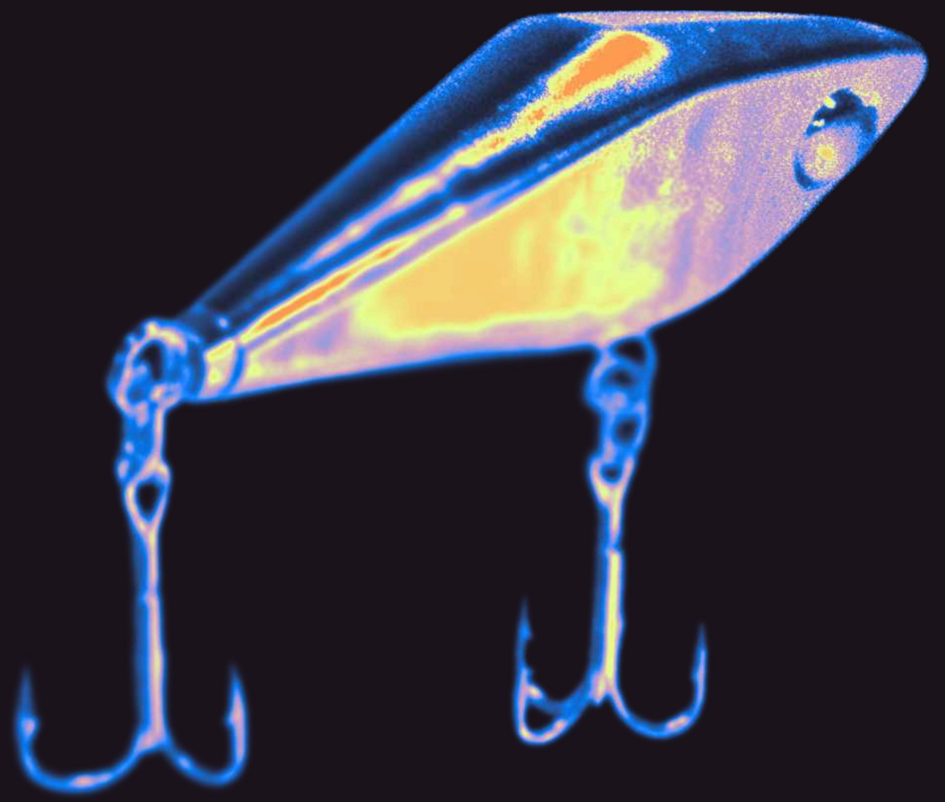
The Recruitment Scam Funnel

How attackers exploit the high-trust environment of the hiring process

STAGE 1

The Lure

A polished, AI-generated LinkedIn profile for a recruiter at a Fortune 500 company.



STAGE 2

The Engagement

Chatbot-driven conversation that builds rapport over a few hours or days.

STAGE 3

The Trap

A 'technical assessment' link is sent. It looks like a coding environment, but it's a drive-by download for InfoStealer malware.

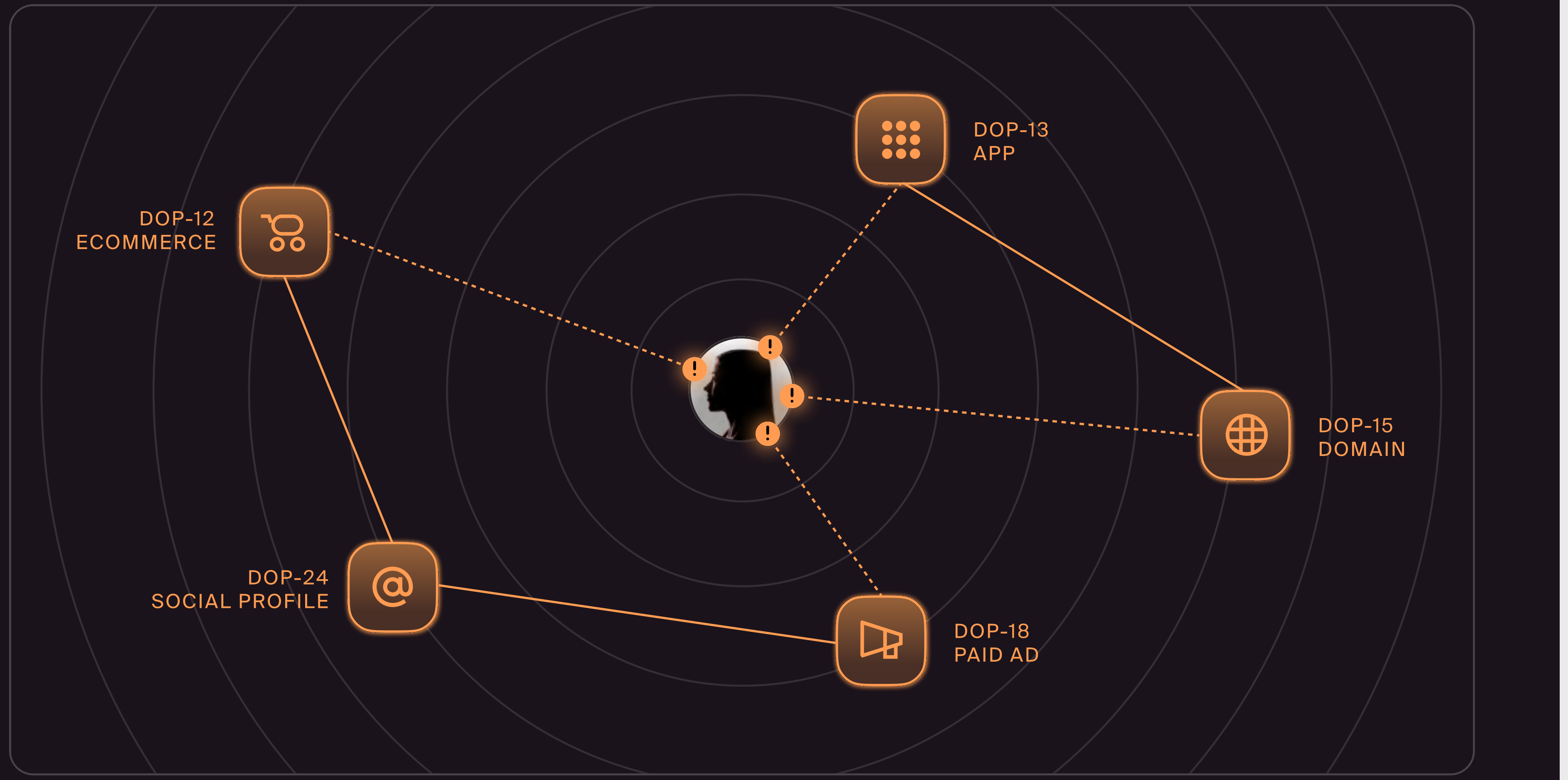
The multi-channel siege

ATTACKERS MOVE LATERALLY ACROSS PLATFORMS

Traditional security assumes attacks happen in silos. Email security watches email. Web gateways watch URLs. Brand protection watches domains. Attackers know this, and they've designed their campaigns to exploit these gaps.

> By 2026, the majority of sophisticated campaigns will move beyond single-channel attacks to become multi-channel by design, utilizing a web of connected assets to evade detection.

If an attacker uses paid ads, social media, and email in tandem, they can reach more people across multiple channels.



Doppel's internal analysis of recent campaign data reveals the extent of this coordination:

45%
of all identified campaigns are multi-channel

16%
of campaigns combine Social Media + Paid Ads

15%
of campaigns specifically combine Domains + Paid Ads

Consider an attack that starts with a paid ad on a social media platform (bypassing email filters). The ad leads to a spoofed domain (which is brand new and not yet flagged). The domain encourages the user to download a file or enter credentials.

If your security team is only looking at one of these vectors, they miss the pattern. The attacker relies on the fragmentation of your defense.

As attackers continue preying on fear and empathy to prompt instant reactions across channels, organizations will adopt their own authentication protocols. They'll use secret code words and recognize subtle cues, such as when, why, and how someone typically communicates.

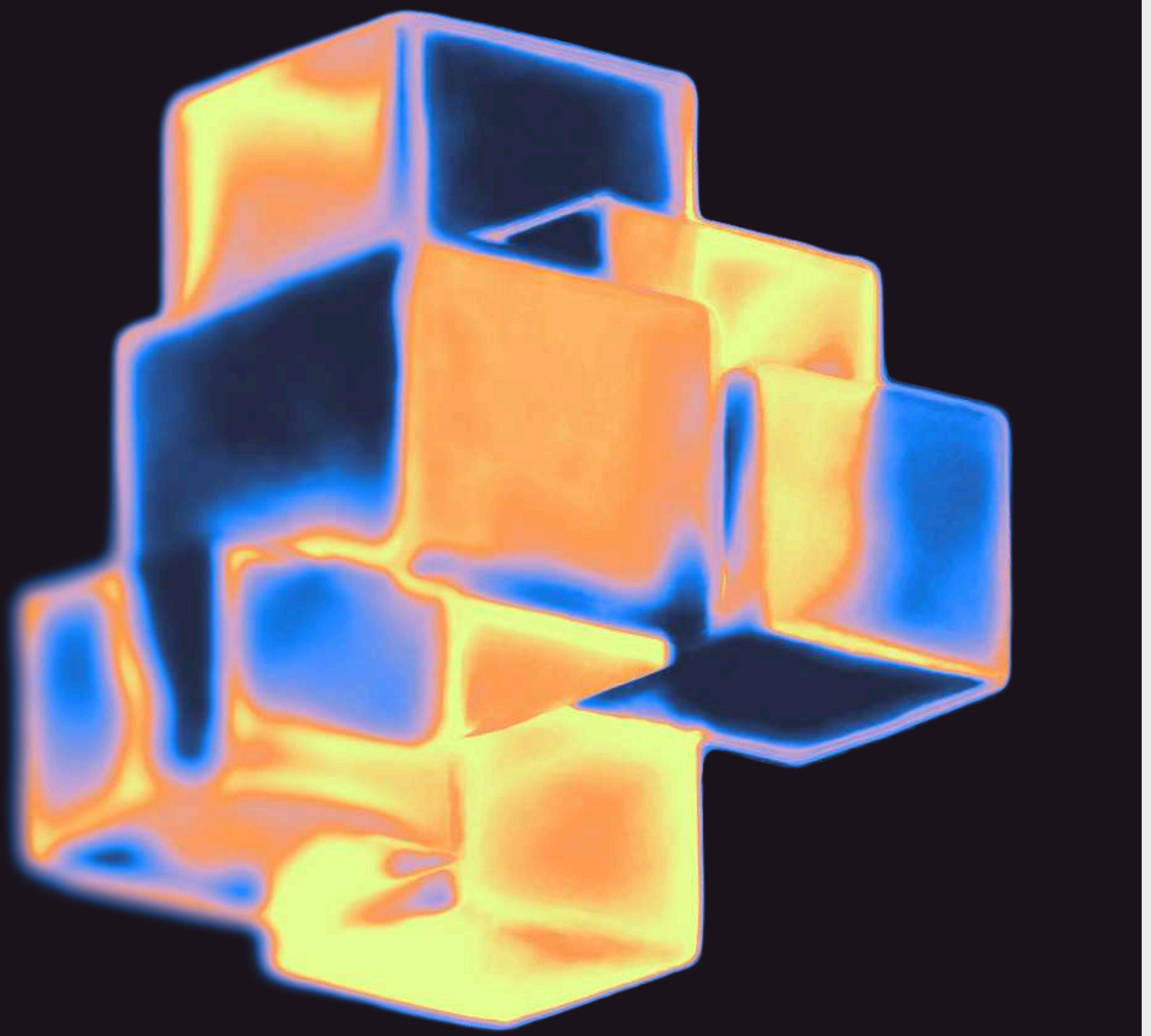
This 'Code Word Society' will become second nature as workforces pay close attention to cadence, context, and tone. When a call or message feels unusually urgent or out of character, the safest next step will be to pause and verify before engaging.

The agentic future

AI VS AI: THE NEW FRONT LINE

The volume of threats is outpacing human capacity. When an attacker can use AI to generate 1,000 unique phishing sites in the time it takes an analyst to put together one takedown request, the math of defense collapses.

The most effective way to keep up with these attacks is to use an AI-powered approach, because the volume and velocity of modern deception demand defenses that think and act autonomously.



Speed is Survival

Human response times, measured in hours or days, are insufficient. Defense must act in seconds. AI-equipped teams detect and contain incidents nearly 100 days faster than teams without AI.[6]

Cost of Inaction

The financial gap is widening, and organizations using security AI and automation save an average of $1.9 million compared to those that don't.[7]

Continuous Learning

AI agents will detect, verify, and neutralize campaigns while continuously learning from every takedown.

Loop

Human analysts will move up the stack, guiding the strategy while AI agents handle the tactical warfare of detection and disruption.

Doppel has already begun this shift. By automating the detection and remediation process, we've enabled our customers to resolve threats 5x faster than they could with manual processes.

< 13 HOURS	~3 HOURS	~65+ HOURS
Doppel resolution time across domains, paid ads, and social media	Doppel mitigation of credential theft domains	Industry manual average

Social engineering defense in 2026

The predictions for 2026 present a stark reality: Digital trust is fractured, media is manipulable, and deception is automated.

Legacy digital risk protection vendors can’t defend against this reality. They were designed for an era of infrastructure protection, not social engineering defense. They look for ‘bad code’ while the attacker is exploiting human trust.

Unlike those legacy vendors, who often provide alerts without action or limit their scope to traditional channels, Doppel focuses on rapid, automated takedowns across the entire digital ecosystem.

Doppel is the AI-native platform designed for this new era. We’ve pioneered the category of social engineering defense. We don't just flag artifacts; we dismantle the underlying infrastructure.

1. Unify Threat Intelligence

We see the whole attack. By ingesting data across the dark web, social media, domains, SMS, and paid ads, we detect the multi-channel patterns that single-point solutions miss.

2. Automate Takedowns

We fight automation with automation. Our AI agents handle the takedown process at scale, removing malicious content before it can gain traction.

3. Simulate Attacks

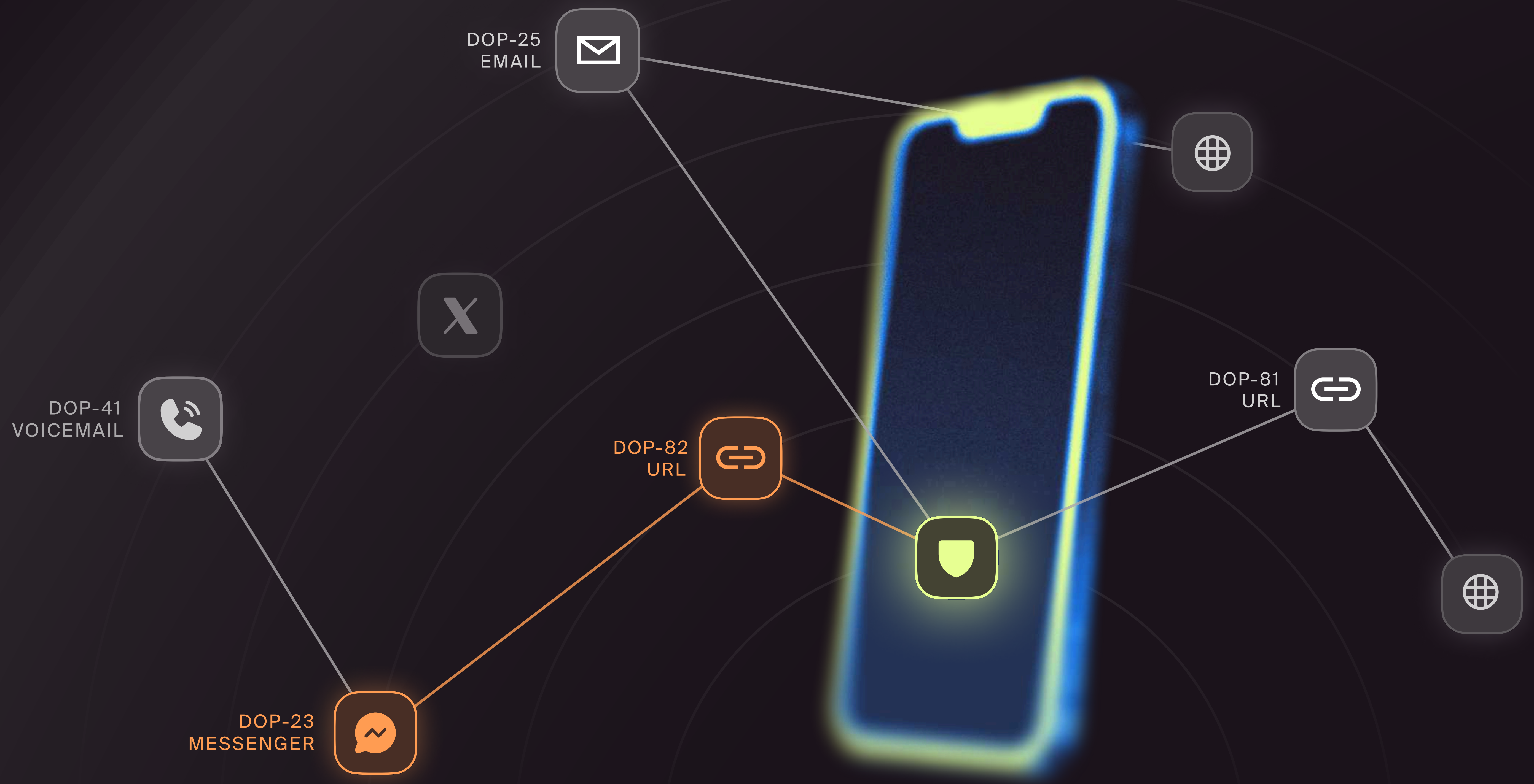
We inoculate your workforce. Doppel actively trains your employees against the very threats we detect in the wild, using safe, simulated campaigns and training to build human resilience.

Doppel

The time to detect is shrinking. And the time to disrupt needs to shrink faster.

Every security leader must ask: Is our organization built to disrupt deception, or only detect it?

Request a demo today



[1] HTTPS://WWW.VERIZON.COM/BUSINESS/RESOURCES/REPORTS/DBIR/

[2] HTTPS://WWW.ENTRUST.COM/COMPANY/NEWSROOM/DEEPFAKE-ATTACKS-STRIKE-EVERY-FIVE-MINUTES-AMID-244-SURGE-IN-DIGITAL-DOCUMENT-FORGERIES

[3] HTTPS://ABOUT.LINKEDIN.COM/TRANSPARENCY/COMMUNITY-REPORT

[4] HTTPS://WWW.FTC.GOV/NEWS-EVENTS/DATA-VISUALIZATIONS/DATA-SPOTLIGHT/2024/12/PAYING-GET-PAID-GAMIFIED-JOB-SCAMS-DRIVE-RECORD-LOSSES

[5] HTTPS://WWW.RESEMBLE.AI/VOICE-CLONING/

[6] HTTPS://WWW.IBM.COM/THINK/INSIGHTS/WHATS-NEW-2024-COST-OF-A-DATA-BREACH-REPORT

[7] HTTPS://NEWSROOM.IBM.COM/2025-07-30-IBM-REPORT-13-OF-ORGANIZATIONS-REPORTED-BREACHES-OF-AI-MODELS-OR-APPLICATIONS,-97-OF-WHICH-REPORTED-LACKING-PROPER-AI-ACCESS-CONTROLS

©2026 DOPPEL INC.