



GASA Scam Fighter Award

GASA

The GASA Scam Fighter Awards recognize excellence in combating scams across prevention, detection, disruption, and enforcement.

Award categories

Recognising impactful efforts across policy, collaboration, technology, awareness and research.



Awareness or Education

Public campaigns, training initiatives or educational efforts that increase scam awareness and consumer resilience.



Cross-Sector Collaboration

Partnerships between government, private sector, NGOs or international bodies demonstrating coordinated action against scams.



Investigation or Research

Analysis or research initiatives that uncover trends and provide insights to support prevention, detection and enforcement.



Policy or Regulatory Initiative

Legislative frameworks, regulatory measures or government programmes that effectively combat scams and strengthen enforcement.



Technological Solution

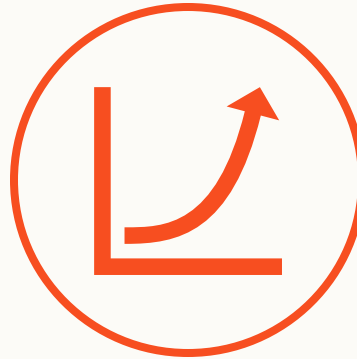
Software, platforms, AI tools or technical innovations that prevent, detect or disrupt scam activity.

Nomination Criteria



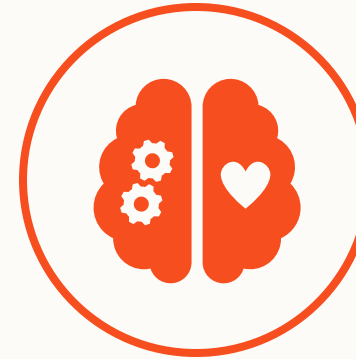
Impact

Ability to increase scam costs, reduce success rates or improve enforcement outcomes.



Scalability

Potential for adoption across sectors, countries or regions, and the extent to which others can replicate or learn from the initiative.



Innovation

Level of originality, forward-thinking approach and effectiveness of the solution or initiative.

Our Scam Fighter Awards Jury



Paul Benda

Executive Vice President Risk, Fraud &
Cybersecurity
American Bankers Association



Matt Noyes

Cyber Policy & Strategy Director
US Secret Service Office of Investigation



Justen Davids

Global Public Policy & Industry Relations
SOMOS



Melissa Lanning

Executive Director
BBB Institute for Marketplace Trust



Laureen Kapin

Deputy Director for International
Consumer Protection & Privacy
Federal Trade Commission



Brian Cute

CEO
Global Cyber Alliance

Let the Pitches Begin!

GASA

Best Awareness Campaign or Educational Program

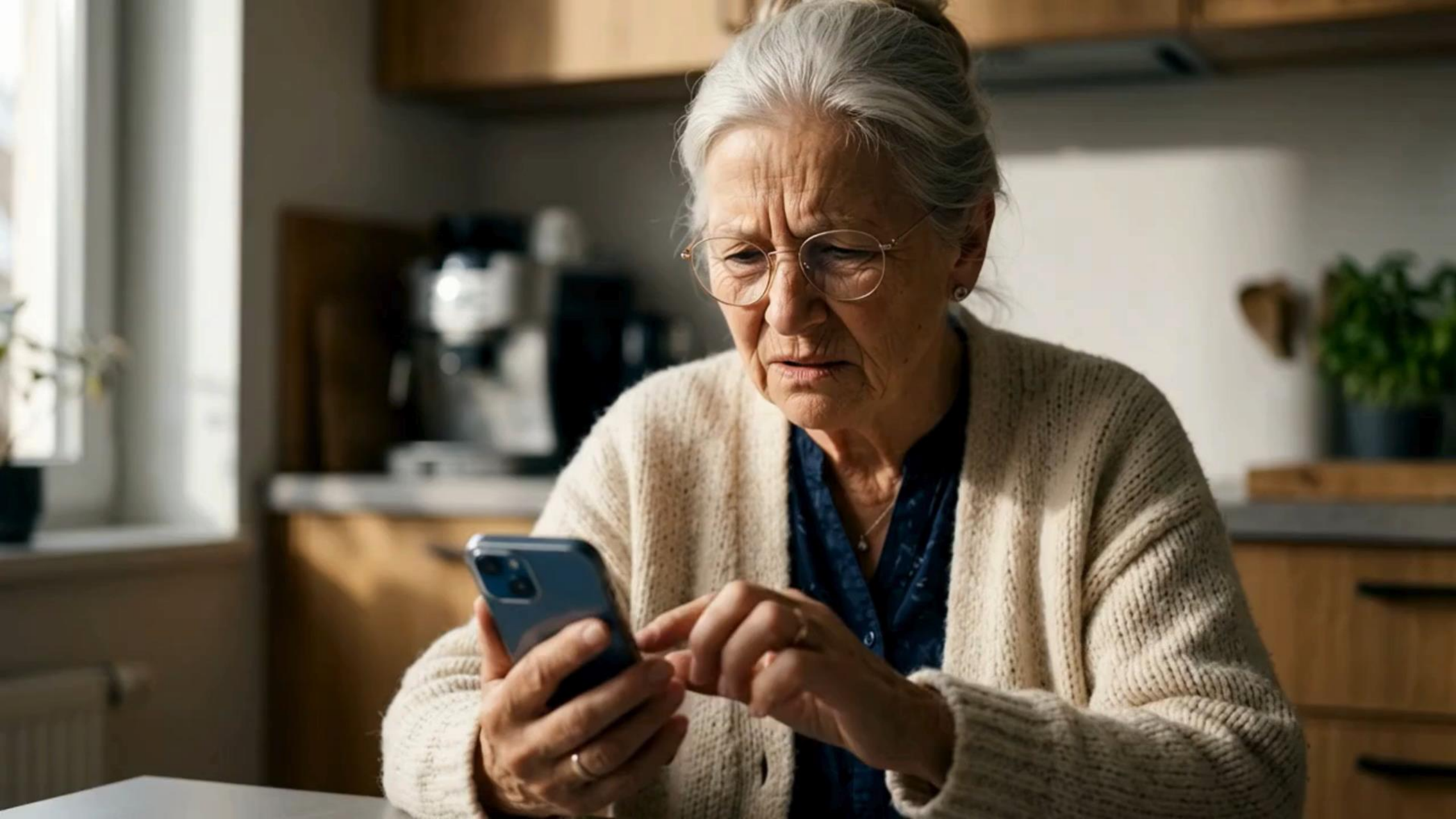


Bitdefender®



Scan to Vote!
(you can only vote once)

GASA



Best Cross-Sector Collaboration



Scan to Vote!
(you can only vote once)

GASA

6 minutes

That's how long it takes a phishing site to go from creation to scam messages landing on devices.

SMS

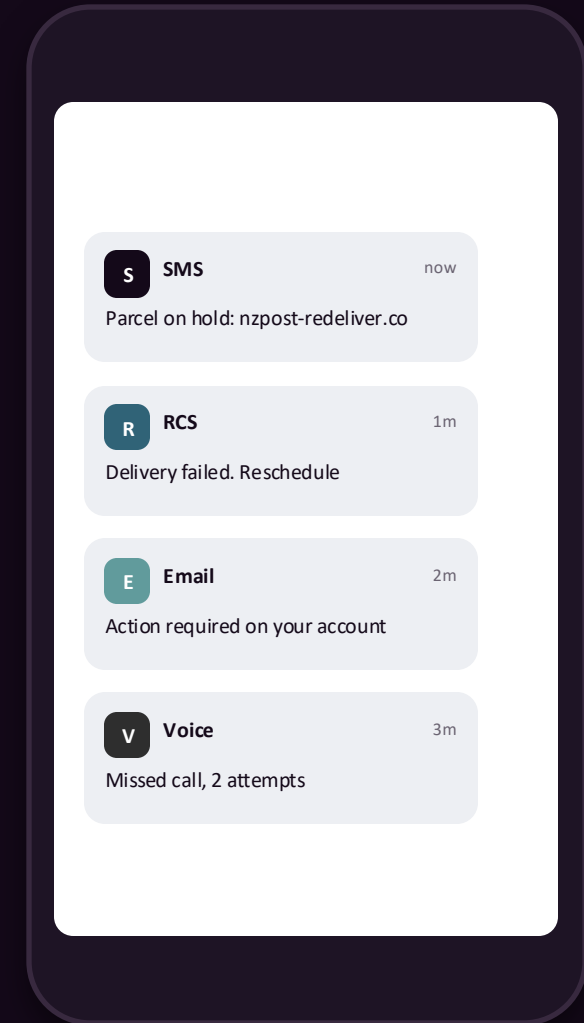
RCS

EMAIL

VOICE

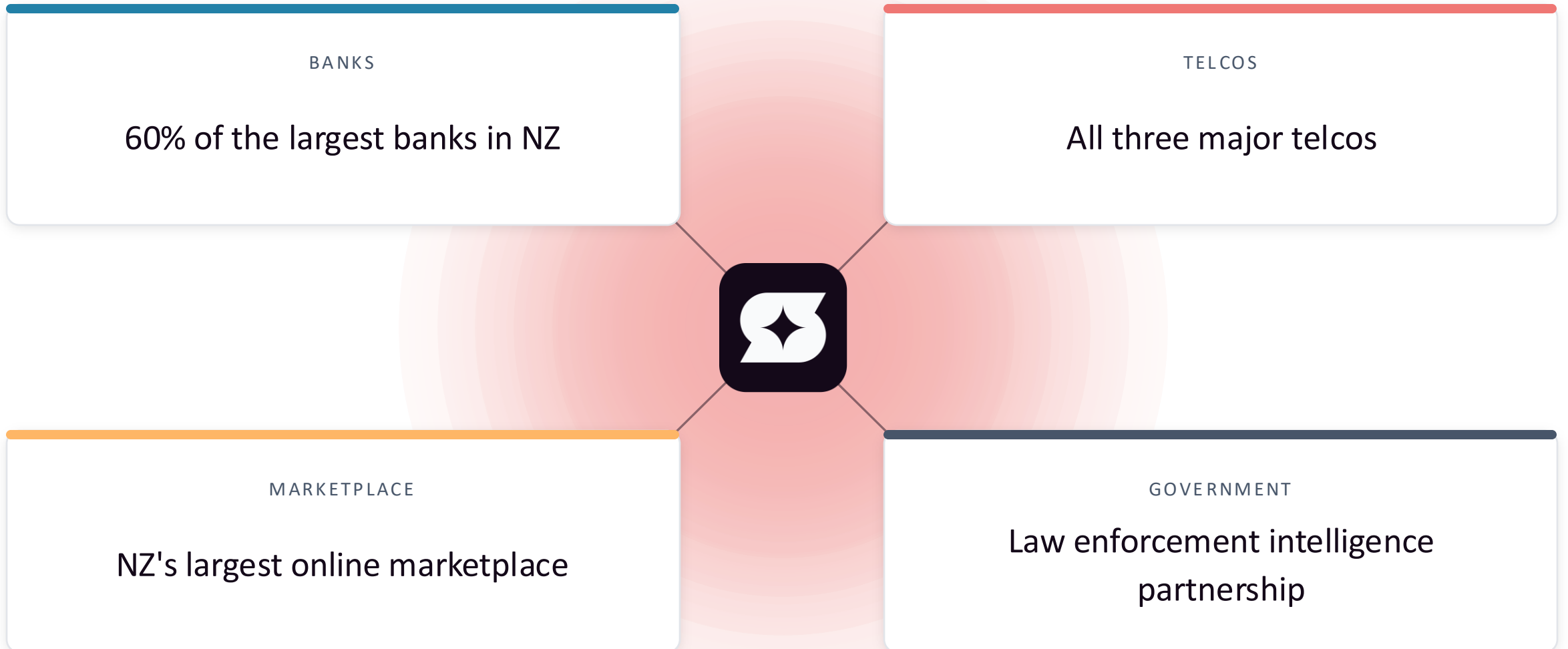
QR

DIGITAL PLATFORMS



Banks. Telcos. Government. Marketplace. FraudTech. One shield.

"Fraud is a collective problem, and collaboration supercharges our collective defence."



\$23.8M

consumer losses prevented
(\$NZD)

\$23.8M

consumer losses prevented
(\$NZD)

23,019

malicious sites blocked

3.1M

attempts to access malicious sites
sites

80%

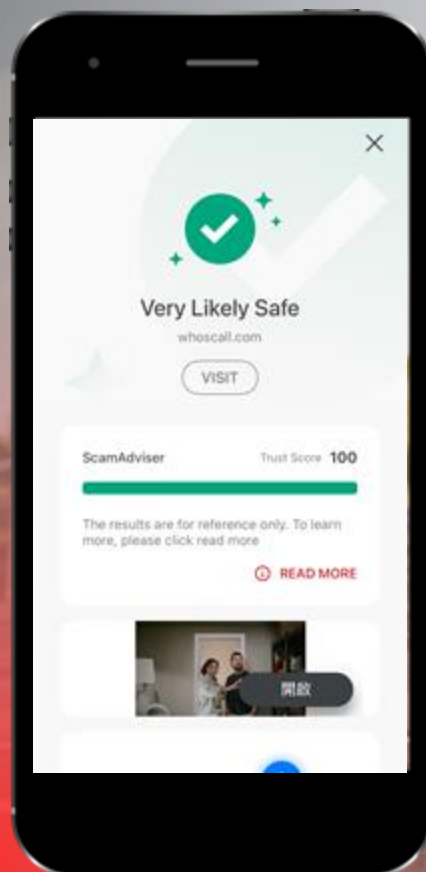
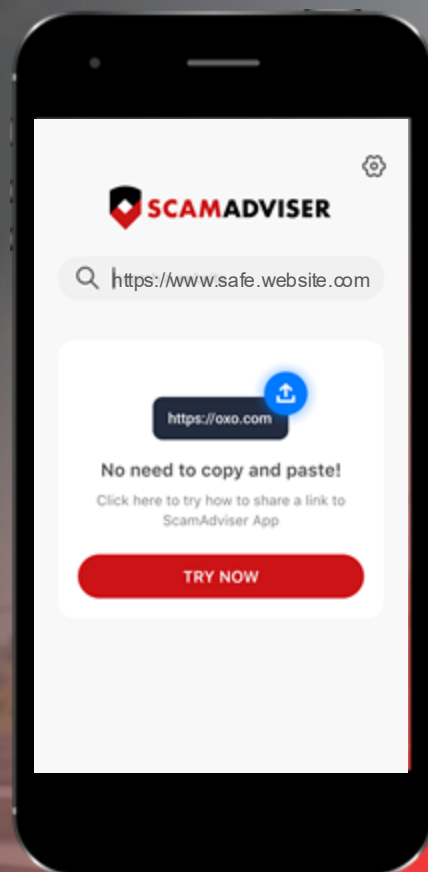
of NZ internet protected

0

false positives reported

A new model for national fraud disruption.

How collaborative disruption shifts the dial.





Kateryna Shinkarenko

Sponsored

Library ID: 5992985420760871

QuantumAI

Do you want
to earn 3,500 euros
a day?



Alekseeva Vasilisa

Sponsored

Library ID: 556156889902095

98% of people have successfully invested and are happy with the results.

\$269

Their algorithm makes \$ 1,500 in 5 hours
on the rise and fall of cryptocurrencies.

Play

0:11 / 0:28

INNOVATIONPR1560OBJECTC.TECH

Alekseeva Vasilisa

Learn more



Finace

Watchmen

The Infrastructure for
Digital Trust

Scam Ads Detection & Classification



LAYER 01

Keyword screening & multi-signal dynamic detection



LAYER 02

Expert Rule Engine



LAYER 03

LLM Semantic Analysis



LAYER 04

Regulatory Compliance Pre-Classification



**Flagged,
Report &
Takedown**

FROM

Taiwan Central Government & Financial Regulators



Intercepting investment scams and reporting scam ads & websites

TO

Taiwan Local Government & Agricultural Sector



Eliminating agri-product scams to safeguard farmer livelihoods in Yunlin

National-Level Defense: Proven Impact with Government Authorities

▼ 38%

Drop in investment scam share of
total financial losses

▼ 50%

Cut in investment scam prevalence

<8hrs

Detection-to-takedown speed
*Down from Weeks



Best Investigation or Research



IJM

tunic **PAY**



Scan to Vote!
(you can only vote once)

GASA

19AUG25

Examining a nexus between the financially-motivated

SEXTORTION OF CHILDREN & FORCED SCAMMING

Funded by:

 Safe Online

 Thomson
Reuters™

*stock image, not a survivor

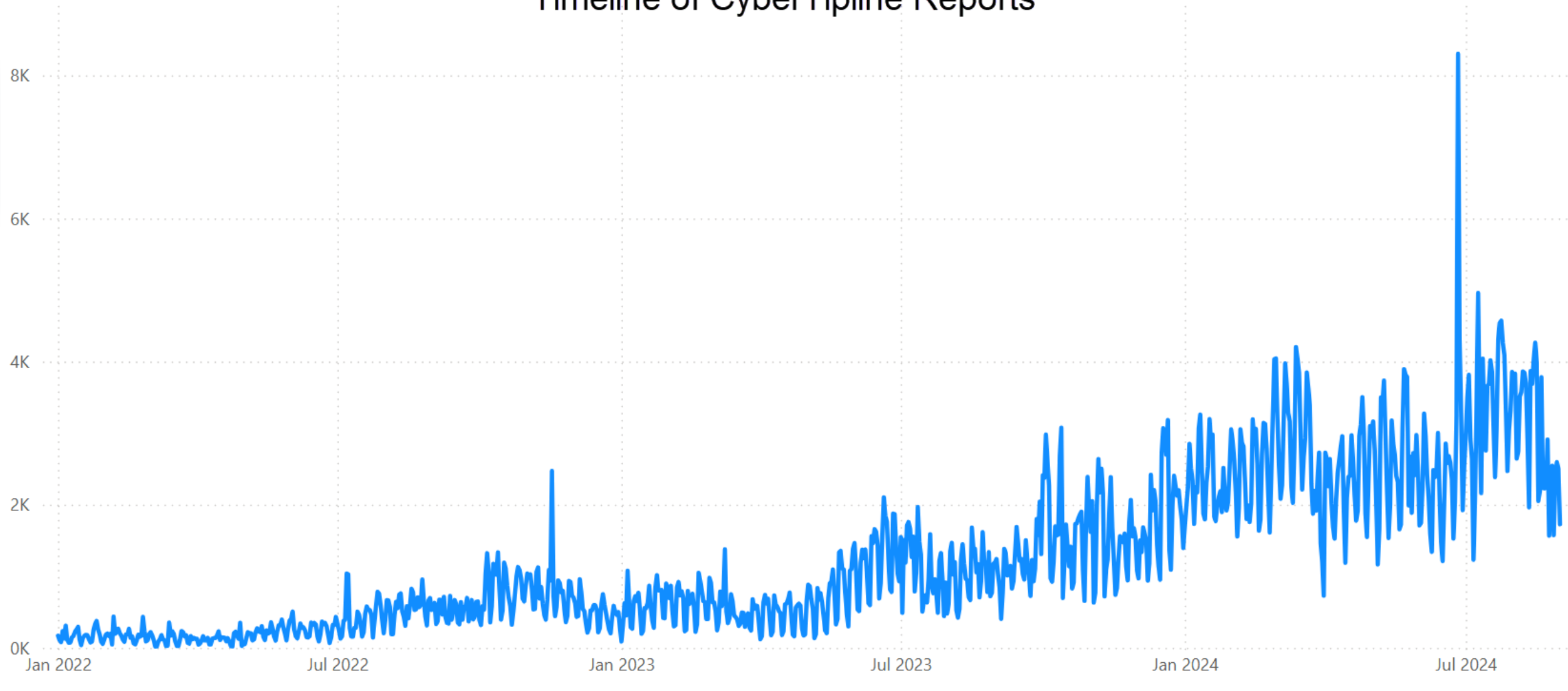


CyberTipline Reports **OVER 1 MILLION**

Categorized as Online Enticement

From January 2022 through August 2024

Timeline of CyberTipline Reports



Timeline of Online Enticement CyberTipline Reports by date report was received by NCMEC (UTC).

SOUTHEAST ASIA

27K

CyberTipline Reports

Attributed to Cambodia, Laos,
Myanmar, and Thailand

85K

IP Addresses

From the CyberTipline
Report data



ADVERTISER ID DATA

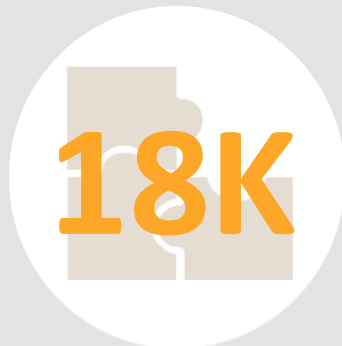


LOCATIONS
known to be associated
with Forced Scamming



300M
ROWS OF DATA

with IP addresses, location data, and
date/timestamps



CYBERTIPLINE
REPORTS

connected through matching
IP addresses

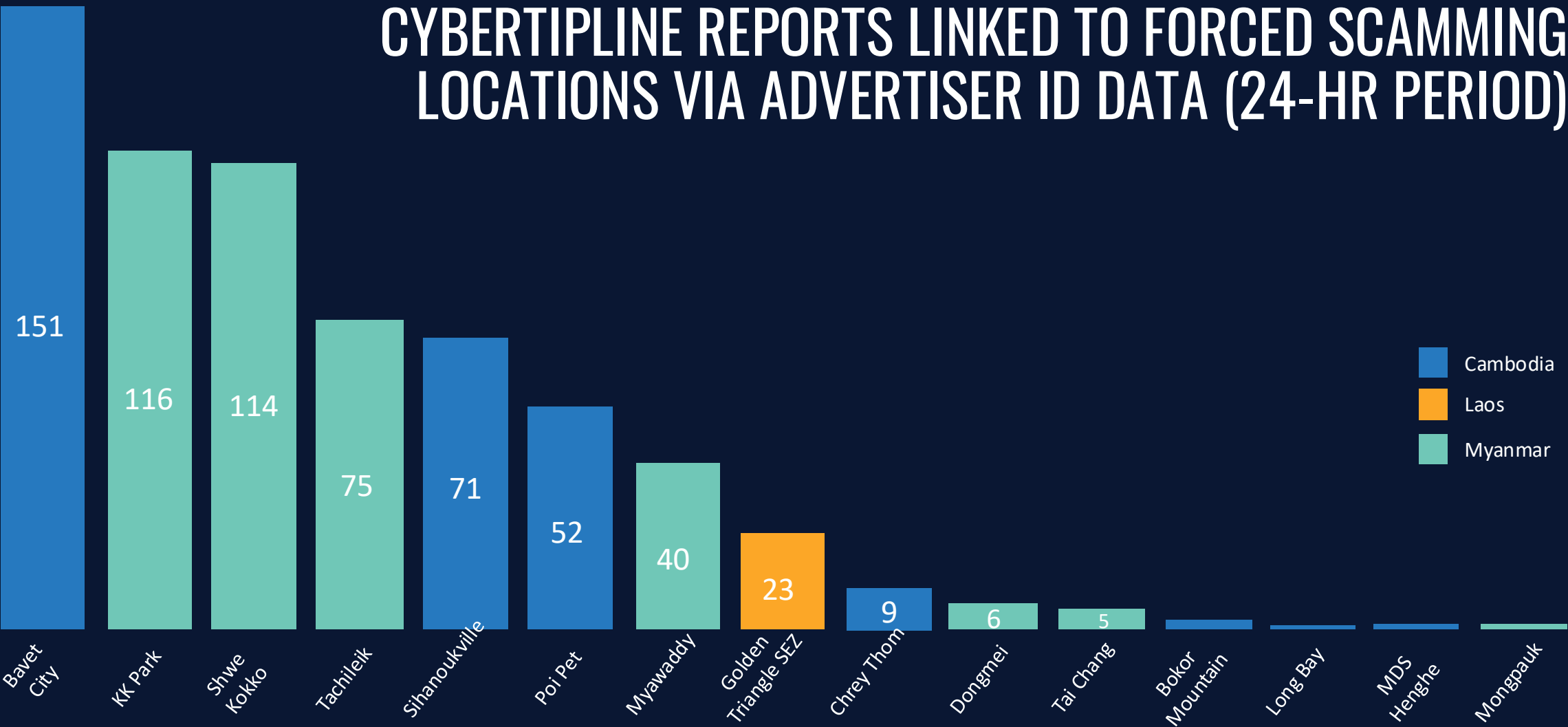
CyberTipline Reports

493

Linked to Forced Scamming Locations

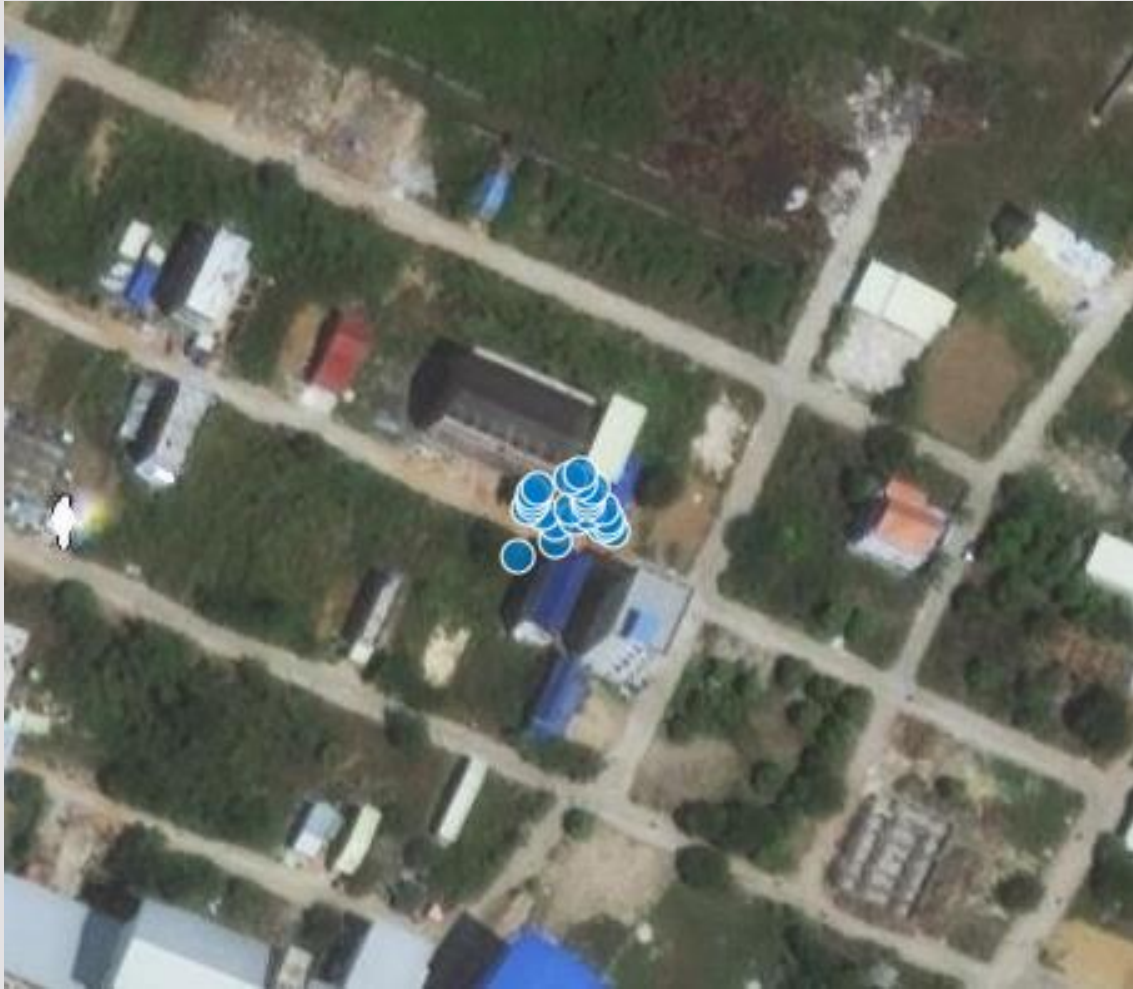
After comparing internet connection timestamps
within a 24-hour period.

CYBERTIPLINE REPORTS LINKED TO FORCED SCAMMING LOCATIONS VIA ADVERTISER ID DATA (24-HR PERIOD)





KK Park, Myanmar



Poi Pet, Cambodia



Myawaddy, Myanmar

RECOMMENDATIONS

IJM urges governments, law enforcement, and tech companies to:



RECOMMENDATION 1

INVESTIGATE FURTHER



RECOMMENDATION 2

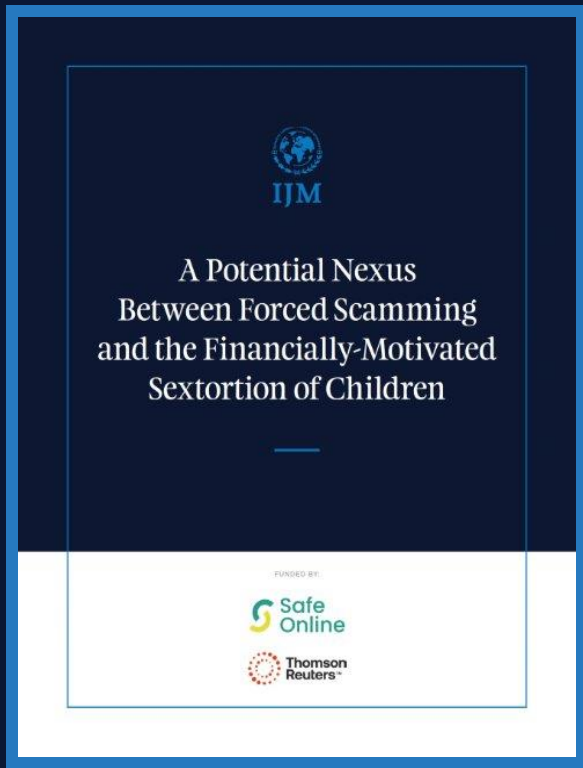
DISMANTLE THE NETWORKS



RECOMMENDATION 2

PROTECT VICTIMS AT RISK

READ THE REPORT



<https://www.ijm.org/nexus-report>

nexus@ijm.org

SCAM FIGHTER AWARDS 2026 · BEST INVESTIGATION OR RESEARCH

Scam-free Agentic Commerce

Tunic Pay, counterparty intelligence, live inside the fraud operations of the biggest banks. We verify who the customer is paying.

>\$25m

<1%

MASTERCARD'S OPEN QUESTION TO US

Every protocol verifies the agent. Nobody verifies the payee.

Layer 1	Consumer → Agent	Did the customer actually ask for this? <u>Know Your Agent</u>	✓ covered
Layer 2	Agent → Issuer	Does the agent have permission to spend? <u>Order Intent & Consent</u>	✓ covered
Layer 3	Agent → Network	Is this a trusted, registered agent? <u>Interface Standards</u>	✓ covered
Layer 4	Agent → Merchant	Is the payee legitimate? <u>Tunic Pay's Verification Layer</u>	• OPEN · this is us

"Trusted Agent Recognition confirms the agent is legitimate. Whether the merchant is legitimate is unspecified – an open area for the industry." Mastercard

WHAT WE DID · WHAT WE FOUND

We became the attackers, and found four ways in

Every other layer is about the agent and the customer. This layer is about the payee.

PATTERN 1

Impersonation

A lookalike storefront and seller-agent mimicking a brand you trust, the agent matches on name, not identity.

PATTERN 2

Prompt injection

Hidden, agent-directed text on the page, engineered to steer a visiting shopping agent's decision.

PATTERN 3

Phantom merchant

A storefront that exists only to capture the payment, no goods, no recourse. The classic purchase scam, industrialised.

PATTERN 4

Manufactured reputation

Fake reviews, paid social ads and seeded trust signals that game the agent's "looks legit" heuristic.

From adversarial testing in a tier-one bank sandbox. We demo patterns 1 and 2 live; all four sit in our scam-typology knowledge graph.

Intelligent agentic workflows is only half of the solution.

We are providing the missing shared context.

A scam seen at one institution protects the members of all the others.
Fraud defences run as a cooperative.



Reasoning

Any frontier model. Rented by the token

Agent workflows

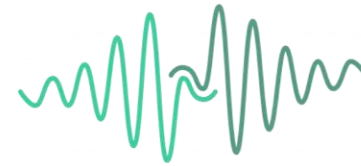
Easily replicated in months

Tunic Pay's shared
payee insights

We have architected the UK's first
system to allow real-time data sharing
for fraud detection purposes

Best Technological Solution

PROXYWARE



RESEMBLE.AI



Scan to Vote!
(you can only vote once)

GASA

GLOBAL ANTI-SCAM ALLIANCE · NORTH AMERICAN SUMMIT



We become the victim so people don't.

Nominee — Scam Fighter Award, Best Technological Solution

Proven impact. A genuinely novel method. Already scaling fast.

WHAT IS PROXYWARE

Decoy personas that see the harm — and stop the next victim

Proxyware deploys AI-driven digital personas on physical devices, detecting harm across digital platforms. When a decoy is targeted, Proxyware verifies the threat and reports 100% of what it finds — so the next vulnerable person is protected instead of victimized.

1



Deploy Decoys

100,000+ AI personas — children, seniors, veterans, corporate workers, government employees, and everyone in between.



2



Detect & Verify

Decoys are approached by scams and harmful content; Proxyware confirms the threat in real time.



3



Report Upstream

Findings route through the Digital Trust & Safety platform straight to the platform owner — no data on real victims is ever collected.



4



Harm Removed

Platforms get exactly what they need to locate and take down the harmful activity at the source.

WHY IT'S DIFFERENT

Individual detection for an individualized internet

The internet isn't one thing — every person sees a different internet, shaped by their own cookies, history, and location. That's why industry-standard detection keeps losing: it scans a generic web that doesn't exist. Proxyware doesn't scan from outside — it stands inside, as the exact victim being targeted.



1. Victim Match

The persona is the intended victim.

A senior persona for senior-targeted scams, a veteran persona for veteran-targeted scams, a corporate-worker persona for BEC fraud — each carrying real browsing history, cookies, interests, age, and demographics. Scammers can't fingerprint them as bots, because they don't behave like one.



2. Geography Match

The persona stands where the harm is happening.

Scam campaigns target specific states, cities, and school districts. Proxyware runs on physical infrastructure inside those same locations — not VPNs — so scammers can't geo-fence away from us without geo-fencing away from their own real-world victims.

30.4%

of distinct threats detected across Proxyware's network were seen at exactly one location — no national feed and no single site would have caught them.

Real cookies, real browsing history, real IPs where the victims are. Nothing to fingerprint, nothing to geo-fence away from.

WHAT OUR DATA SHOWS

133.7 million attacks — and the results behind them



133.7M

attacks detected across every protected sector

Only ~15% of digital crime is ever reported nationally. Proxyware collects zero data on real victims while detecting the other 85%.

The inception point of the harm — exactly as the victim sees it



Secure Connection Failed

svn.boost.org Uses an Invalid Security Certificate.
The Certificate is not trusted, because the issuer Certificate is Unknown
(Error Code : sec_error_unknown_issuer)

- This could be a problem with the server's configuration , or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past , the error may be temporary , and you can try again later.

CALL TOLL FREE 1-888-859-0682

***Ship within 24 hours of placing the order

EUR English

Home Fashion 2023 Fashion street style



UP TO 80% OFF EVERYTHING*

PRICES AS MARKED NO CODE NEEDED

SHOP NOW



Overcoat



Woman's Mid-length Patterned



The Girls' Buffalo Plaid



Woman's Casual Turtleneck



The Trendy Leopard Print



The Modern Camo

93%

success rate identifying and removing digital attacks

85%

of threats targeting children disrupted before they reach them

\$351.6M

in attack surface value detected across 13,186 campaigns, all time

THE FLAGSHIP: VIRGINIA, 33 MONTHS IN

14

locations, live since launch

\$82.6M

in lifetime loss disrupted

976

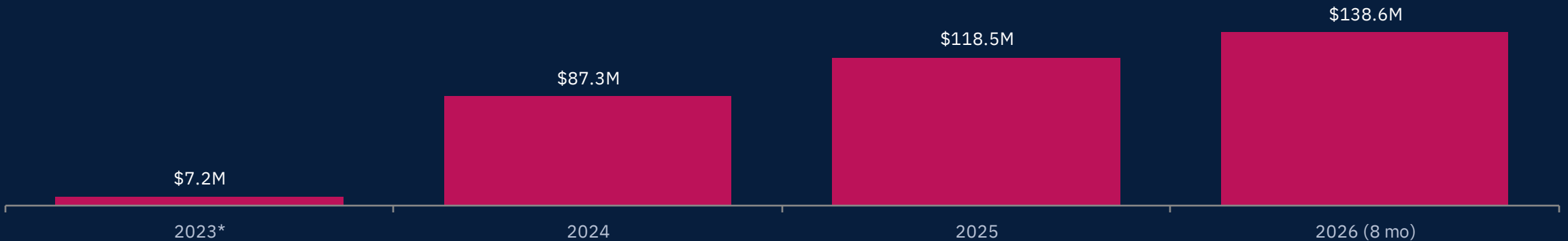
new threats detected in August alone

SCALABILITY

We're not at scale. We're scaling, fast.

7 new states came online in 2026 alone. Each of you plays a critical role, whether you're from law enforcement, a bank, social media, ad tech, or any corporation with a brand, a payment pathway, or a platform scammers can exploit — and the network's own numbers show how fast it can grow to reach you.

ATTACK SURFACE VALUE DETECTED, BY YEAR



*2023 reflects December only, the program's first month — a ~19x increase in attack surface value detected since launch.



TELECOM

Decoys capture the phone numbers behind scam campaigns — ready to route upstream for takedown.



BANKS & CARDS — ABA

Fake storefronts caught before Card-Not-Present fraud drains an account and banks absorb the loss.



LAW ENFORCEMENT

100% of what Proxyware detects is shareable with any level of law enforcement — city to federal.

70+

locations already waiting to join the network, and corporate infrastructure already reaching 120 countries — proof of an architecture built to scale rapidly, anywhere.

Endorsed by LeadingAge Virginia, LeadingAge North Carolina, The Invictus Project, and Edu4life, Inc.



WHY PROXYWARE

Proven impact. A genuinely novel method. A model built to scale.

● IMPACT

133.7M attacks detected and \$351.6M in attack surface value disrupted network-wide, at a 93% success rate — turning invisible harm into upstream reports that raise scammers' costs and cut their success rate.

● INNOVATION

100,000+ victim-matched, geo-matched AI personas — the only model built to stand where scams strike, catching what passive, signature-based detection structurally cannot.

● SCALABILITY

Not at scale yet, but scaling fast: 7 new states in 2026 alone, corporate infrastructure already live in 120 countries, and 70+ more locations ready to come online — one architecture, built to extend anywhere quickly.

Unless this data reaches every company in this room — not just our existing partners — attacks don't stop. They just move. Collaboration is move. Collaboration is how we stop this digital crime epidemic.

PROXYWARE — nominated for the GASA Scam Fighter Award, Best Technological Solution

Thank you.

The world's best AI labs just made fraud effortless

Tedi Papajorgji, CTO, Resemble AI



RESEMBLE.AI

Time to guess: Real or fake?



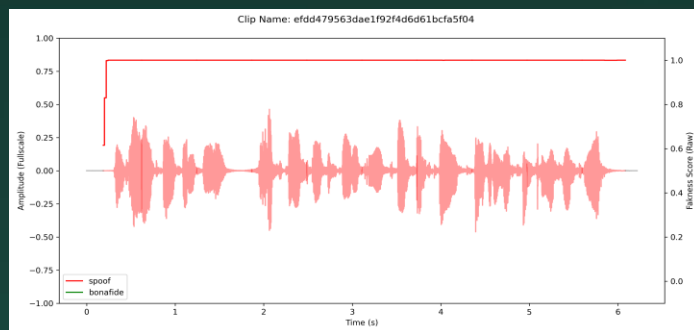
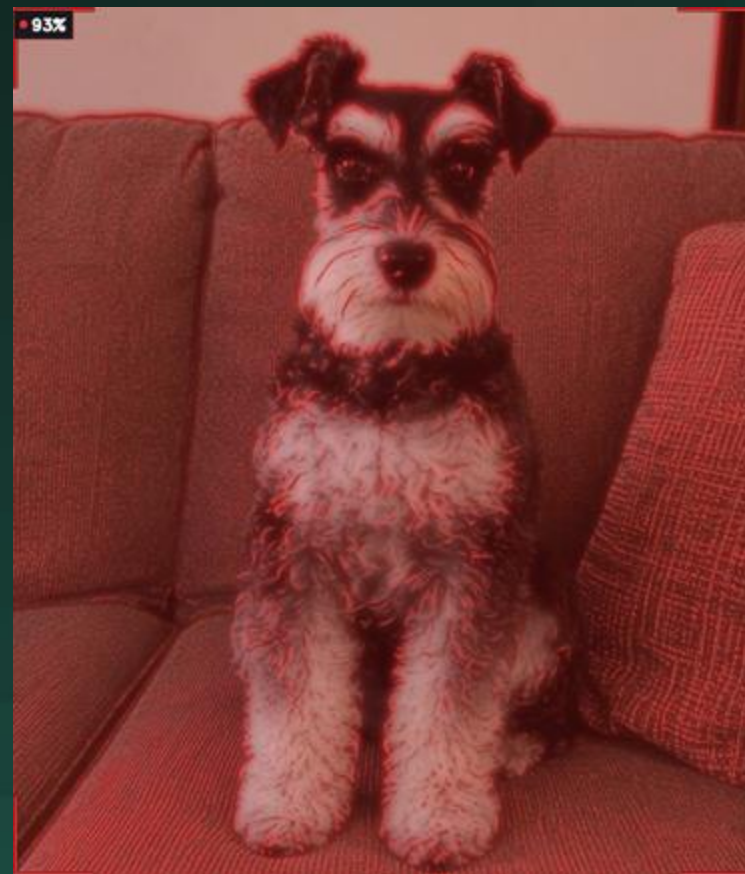
Time to guess: Real or fake?



Time to guess: Real or fake?

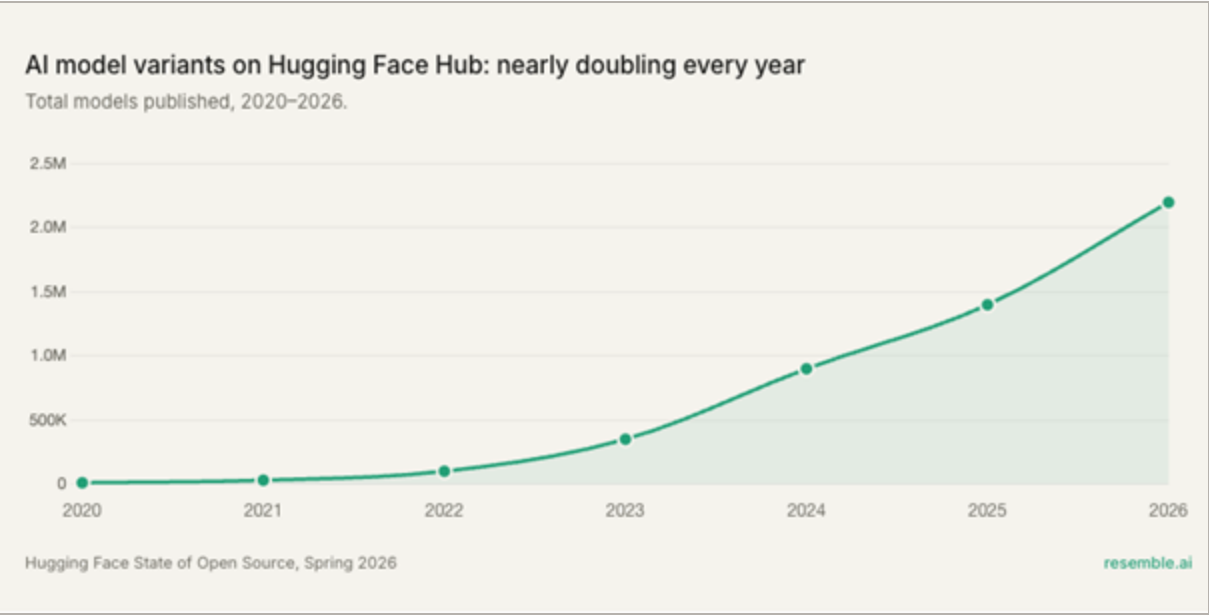


They were all fake. Surprised?



Here's why: World models have come to Gen AI.

Over 2.2 million AI model variants on Hugging Face — nearly **doubling** every year.



August 5, 2025 Models

Genie 3: A new frontier for world models

Jack Parker-Holder and Shlomi Fruchter

[Try Project Genie](#) [Learn more](#) [Share](#)



Alibaba joined ranks of Chinese AI breakthroughs with new Qwen model

Kyiv • UNN • August 3 2026, 12:54 AM • 4454 views

Alibaba introduced the Qwen3.8-Max model with 2.4 trillion parameters, which surpasses Kimi K3 from Moonshot. The new system shows results comparable to Anthropic Fable 5, the export of which was banned by the US.



Everyone is a target.

WhatsApp scam costs Hong Kong man \$1.27 million after criminals used AI voice notes to impersonate his father — experts say secret codewords are the best way to stay safe

News By Alex Blake | Published August 7, 2026

Don't let them steal your savings



1. Consumers

Fraudsters use cloned voices and synthetic video to impersonate family members, bank representatives, and romantic partners — often targeting the elderly.



2. Governments

Deepfake video and audio of public officials is used to spread false narratives, fabricate threats, and generate CSAM at a scale that overwhelms law enforcement.



3. Enterprises

Synthetic voices and faces are used to impersonate executives and account holders, manipulating employees into approving fraudulent transfers and access requests.

Current detection is good, but it's not enough.

Artifact-based detection transformed the field:

- ✓ Trained on known signatures
- ✓ Optimized for speed and precision

What it does well

Precise on known techniques

Fast verdict on recognized generator signatures

Low false positive rate on familiar content

Where it falls short

Misses new generators until retrained

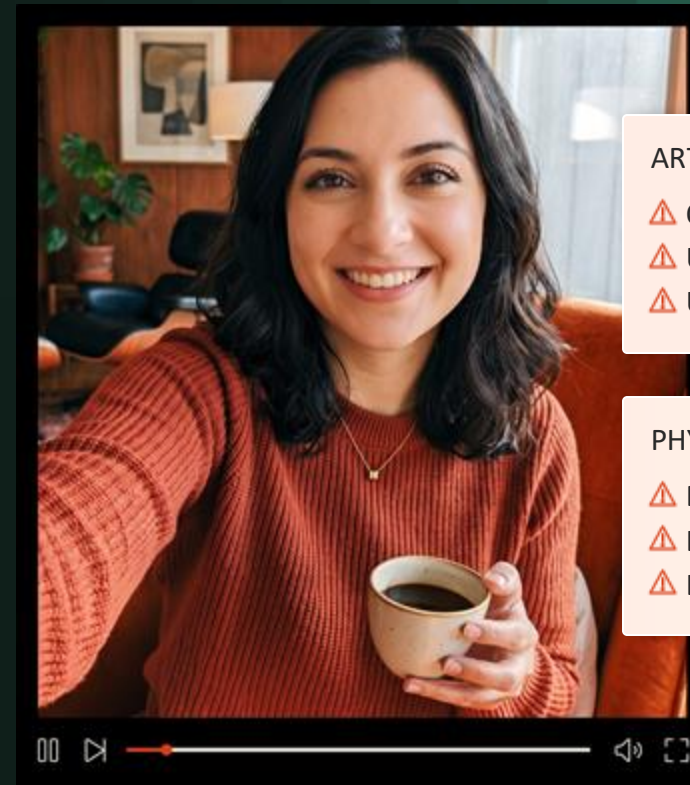
Adversarial fine-tuning can bypass known signatures

The better generative models get, the fewer artifacts they leave for detection

The first detector built to fight world models with a world model

Now asks are there AI signatures —
and do the physics add up?

- ✓ Tested across 250+ generation models
- ✓ Holds up against new generators
- ✓ Multimodal with up to 99.5% accuracy



#1 in audio detection. *Independently benchmarked.*

99.5%

Accuracy

Highest out of a total of 18 systems tested

Third-party benchmark accuracy



BEST IN THE INDUSTRY

0.4%

False negative rate

Critical for fraud, KYC, and authentication where missing a fake is the expensive error.

WELL BELOW 1.0 THRESHOLD

0.12%

Real-time factor

Fits streaming, call-center, IVR, and live voice-agent deployments.

MODERN ATTACK COVERAGE

25

TTS systems tested

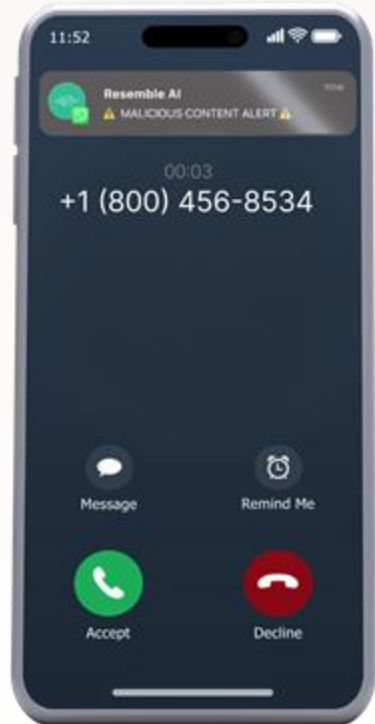
Includes the cloning stack attackers use today such as ElevenLabs, F5-TTS, and Chatterbox.

Source: Podonos Automatic Deepfake Audio Detection Benchmark, 2026 - podonos.com/blog/deepfake-audio-benchmark

A spam filter for digital life

Phone calls

Alerts you when an AI voice is detected on a call.



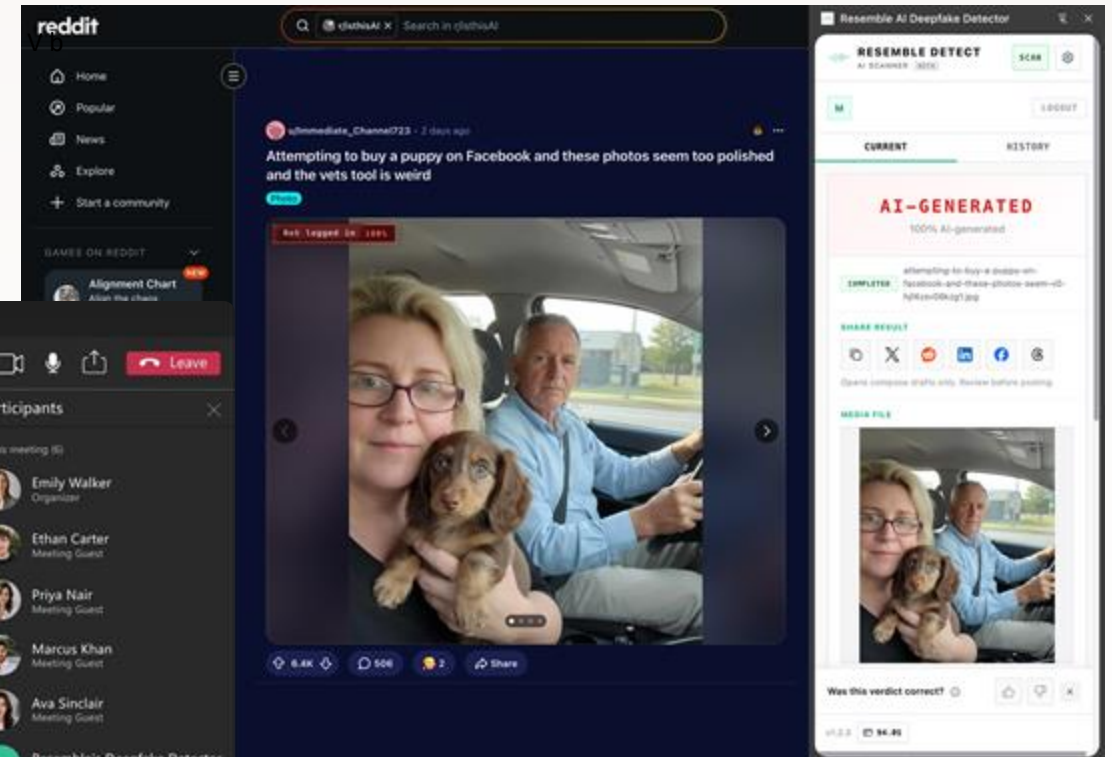
Video calls

Flags deepfakes in real time during live calls.



Browser

Detects AI-generated content while you browse.



Detection is just the beginning

01	Detect: Synthetic detection	REAL-TIME
02	Identity: Likeness ownership	FOUNDATION
03	Verify: Asset ownership	CONTINUOUS
04	Signal: Fraud identification	IN-FLOW
05	Intelligence: Understanding	FORENSIC
06	Trace: Monitor + initiate take-down	PROACTIVE

The layers surrounding detection are what turn model output into decisions an organization can act on, audit, and defend.

Deepfakes are everywhere.
So are we.



RESEMBLE.AI