

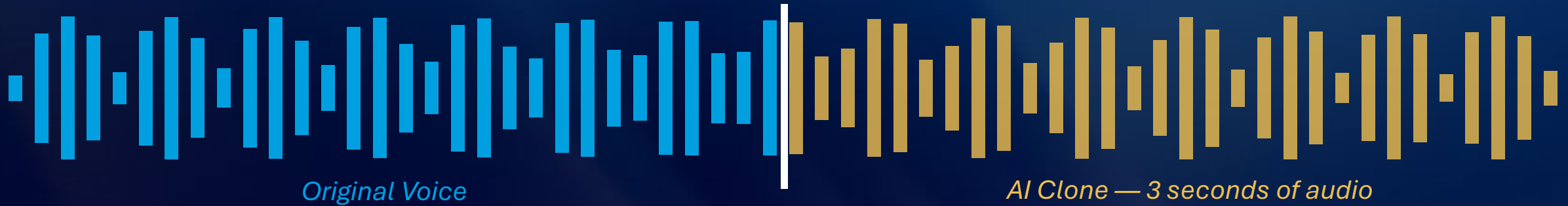
Brake Check: The AI-Powered Threats Your Supply Chain Didn't See Coming



James McQuiggan
Advisory CISO
Apparent Security



3 seconds.



+1,600%

Deepfake vishing surge
Q1 2025 vs end of 2024

Threat Intel 2025

+173%

Deepfake audio in
contact center calls

Pindrop Voice Intelligence Report, 2025

80%

of people fooled by AI
voice clone in study

Nature, 2025



whoami

James R. McQuiggan, CISSP



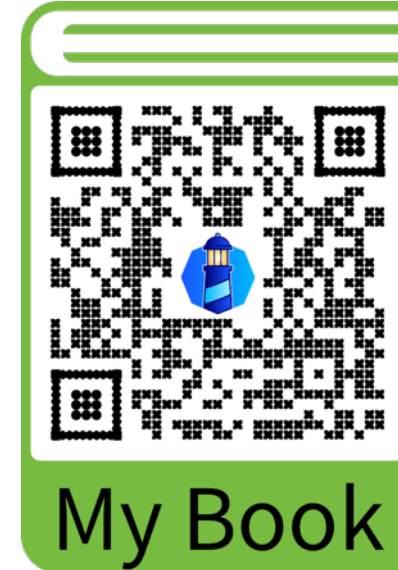
apparentsecurity





whoami

James R. McQuiggan, CISSP



qrto.org
Amazon

LMIEAIA

The AI Threat Landscape



AI Attacks - Internal & External Threats



67% of Employees use Shadow AI

Source: 2026 Verizon Data Breach Incident Report

**URGENT: Route Re-dispatch
& Fuel Authorization**

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam elit
 seditione velle endiment ut a euismod. It expedit ut utrum, effluendum conepit
 recedunt. Donec ornare egestas.

Donec ut ut nunc dolor nunc seditione velle endiment ut a euismod. It expedit ut utrum, effluendum conepit
 recedunt. Donec ornare egestas.

Confirmation link to [Confirmation link](#)

This dispatch order isn't from your dispatcher.

Load Board Phishing: fake listings are the lure

ATTACK VECTOR Email spoofing +
account compromise

SOURCE FBI IC3 public service
announcement

LOSSES \$725M annual

Illustrative load board mock-up (DAT / Truckstop-style listing view)

Age	Pickup	Drop-off	Trip	Equip.	Rate	Broker	Fraud flag
2h	Dallas, TX	Atlanta, GA	780 mi	Van	\$2,150	Lone Star Logistics	
15m	Chicago, IL	Denver, CO	1,000 mi	Reefer	\$5,900	Midwest Freight Grp	FRAUD: rate 45% above lane average
4h	Memphis, TN	Columbus, OH	560 mi	Van	\$1,480	River City Brokerage	
30m	Los Angeles, CA	Phoenix, AZ	370 mi	Flatbed	\$1,900	Pacific Load Co	FRAUD: MC# reactivated 4 days ago, @gmail.com contact
1h	Newark, NJ	Charlotte, NC	620 mi	Van	\$1,850	Garden State Cargo	
20m	Houston, TX	Kansas City, MO	740 mi	Van	\$3,100	ABC Transport Solutions	FRAUD: spoofed broker domain (abc-transp0rt.com)

Training mock-up; companies, rates and flags are fictitious examples of common red flags. Source: FBI IC3 PSA on freight and load board fraud.

AI-Generated BOLs: LLM-written rate confirmations read clean to email filters

Template fraud: caught

- Copy-pasted templates
- Typos and broken formatting
- Wording matches known-bad samples
- **Caught by keyword and similarity rules**

AI-written: gets through

- New document each time
- Lane, rate, PO all correct
- Broker's tone copied
- **Passes filters; a human must catch it**

**Paperwork can no longer vouch for itself.
Verify the sender through a known phone number or portal, not the document.**

Source: EFROS threat tracking, August 2026 (security firm documentation of LLM-generated BOL and rate confirmation bypass).

Trust Breakdown: one stolen account stalls the chain

1

Account compromised

Broker or carrier email login stolen via phishing

2

Trust exploited

Fake rate cons, BOLs and payment changes sent

3

Freight disrupted

Loads diverted or held; payments misdirected

4

Partners stop trusting

Shippers pause tenders, carriers refuse loads

AVERAGE LOSS PER INCIDENT

\$273,990

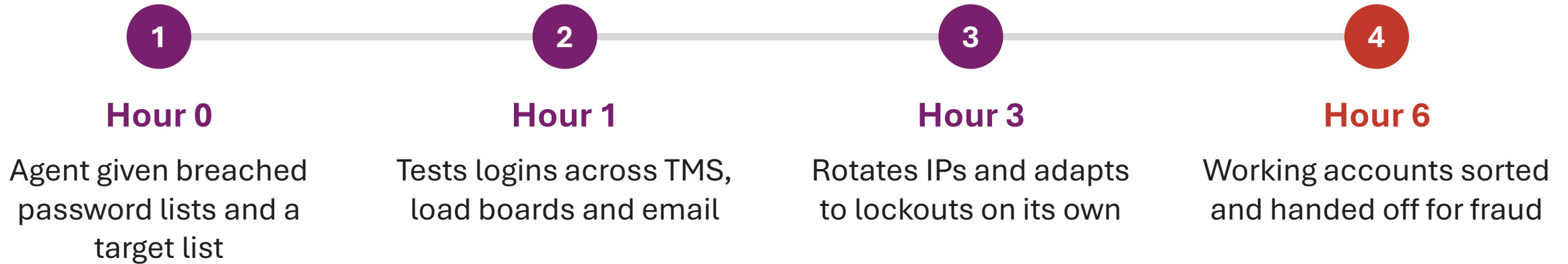
Business email compromise: the same account-takeover pattern that drives load board phishing and fake BOLs.

Sources: FBI IC3 and Verizon DBIR

Source: FBI IC3 annual report; Verizon DBIR. Average loss per business email compromise incident.

Agentic Harvesting: AI steals credentials in six hours

Timeline of one autonomous run, no human operator



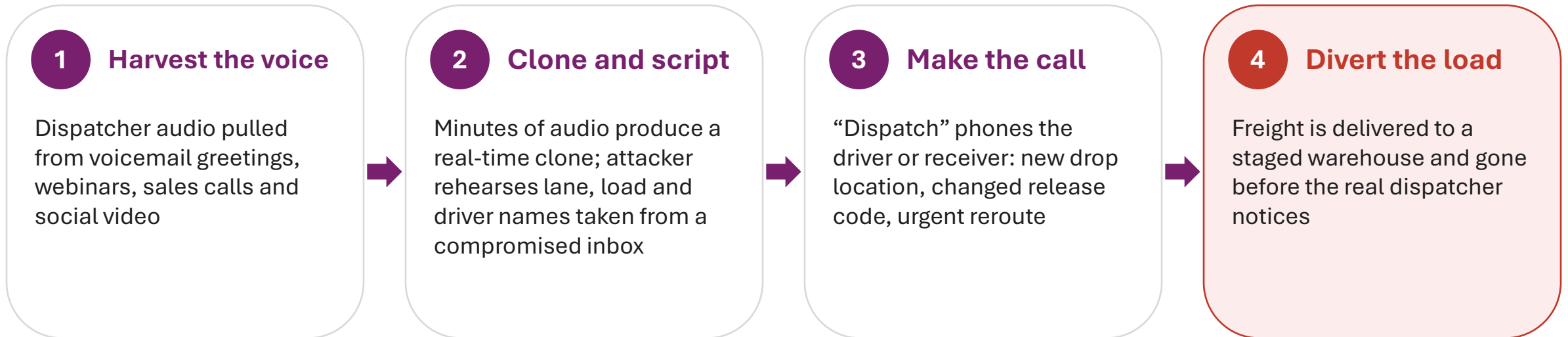
**Reused passwords are found and used before anyone is at their desk.
MFA on every freight system is the control.**



1600% Voice Phishing Increase

Deepfake Dispatch: a cloned voice on the phone moves the freight

Example: operationalized deepfake dispatch calls, how the attack runs



Source: EFROS & NMFTA Threat Report, 2025–2026. Steps are a generalized pattern drawn from reported incidents.



25% Human Deepfake Detection
(Deepstrike, 2025)

Deepfake Video Creation – Head / Shoulders



- Single Image
- Mouth and head movement

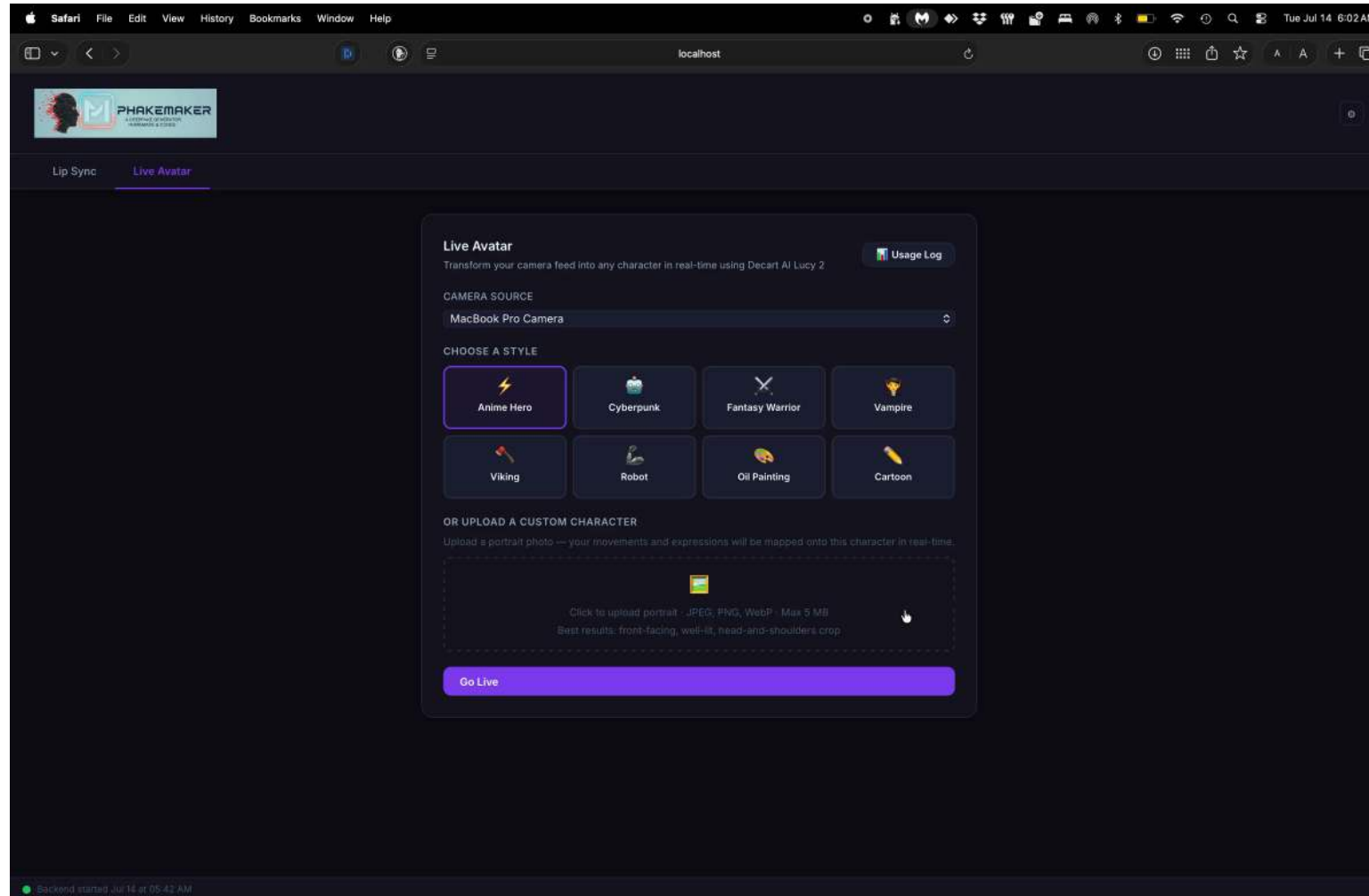


- Video and LipSync
- Video of the target
- Changes the mouth movements to match text



- High end processing
- Swaps face: Hairline, to sideline
- Holding hand in front of face?

Deepfake – Full Body Avatars





Attackers Don't Hack Systems – They Call

Carrier Identity Theft: a stolen MC number is the whole disguise

- 1 Take over the FMCSA record**
Phished portal login; the MC record's email, phone and address become the attacker's
- 2 Look legitimate everywhere**
Load boards and vetting tools now show the attacker's contacts under a clean authority
- 3 Book and double-broker the load**
Fraudster books the load as the real carrier and re-posts it cheaply to an unwitting trucker
- 4 Steal the cargo or the payment**
Freight is rerouted to a staged site, or the honest carrier hauls it and is never paid

Reported carrier identity theft

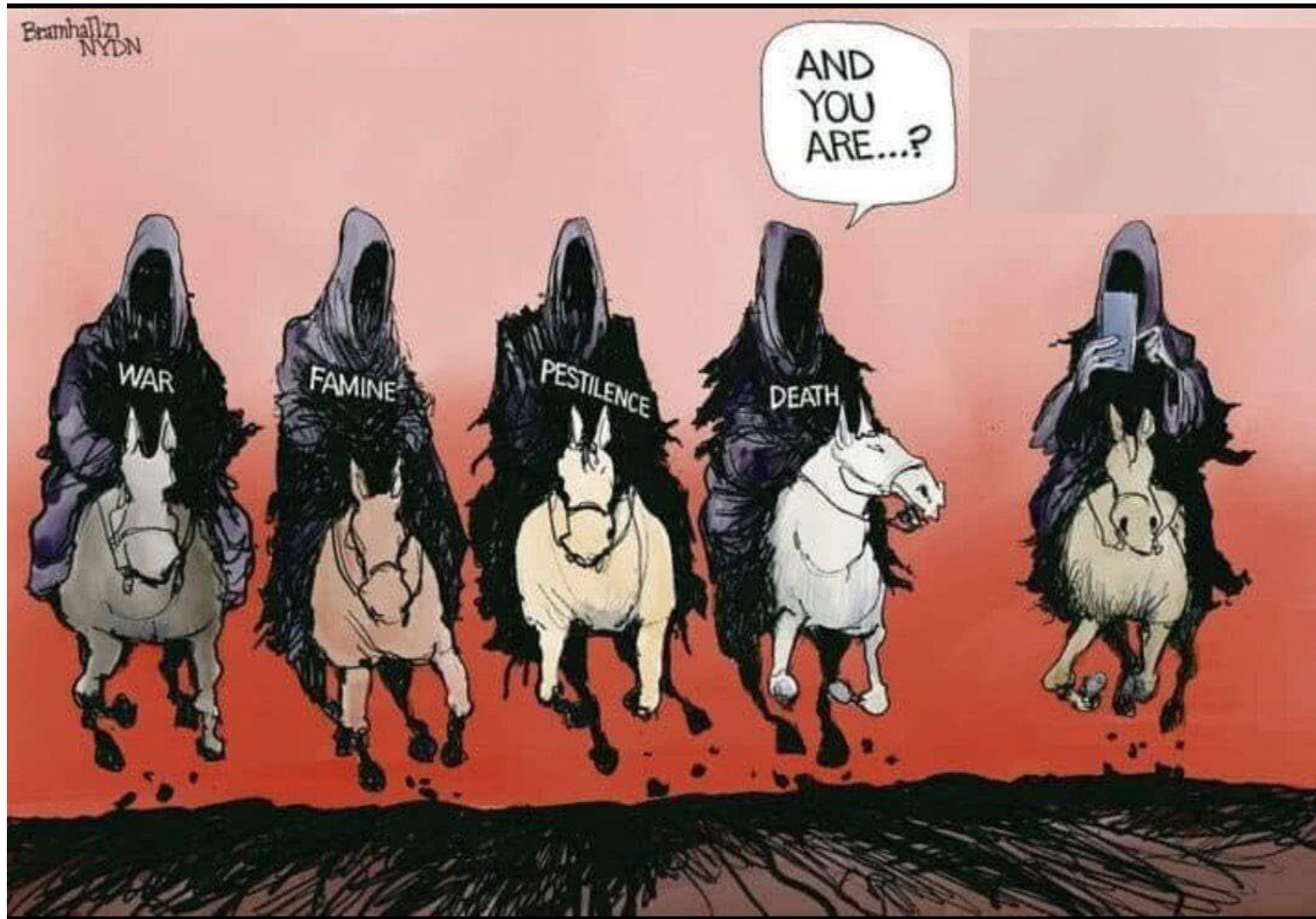
1,475%

growth, 2022 to 2024

Roughly a 16-fold rise in two years

Source: FBI IC3 public service announcement on carrier identity fraud; growth reported for 2022–2024. Steps are a generalized pattern.

Misinformation / Disinformation Campaigns





AI Has Lowered the Bar for Attackers



An Algo-rhythm

Why Training Fails



COMPLIANCE CHECKLIST

HERTACHIDE'S AUDIENCE:



Weigh more responsibility.

And then four very little details, however, before
behavior please have its eyes, they are the same.

This the sort of things a well-known person
resolves, firm and please learn from it.

This letter will be for coming to the
company, an effort, and you can make it.

And then, please, if you are not your
and the same.

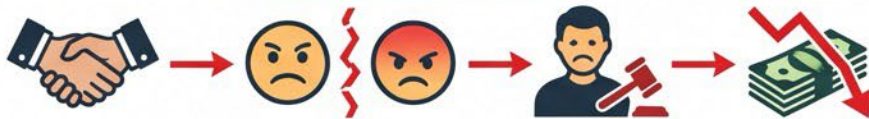
And then, please, if you are not your
and the same.

Compliance Measure Completion Rates
Attackers Measure Click Rates

Trifecta of Gaps

- Training is an event, not a behavior
- Policies protect the organization, not people
- Human are NOT the weakest link!

What's the Costs of Clients Who Lose Trust?

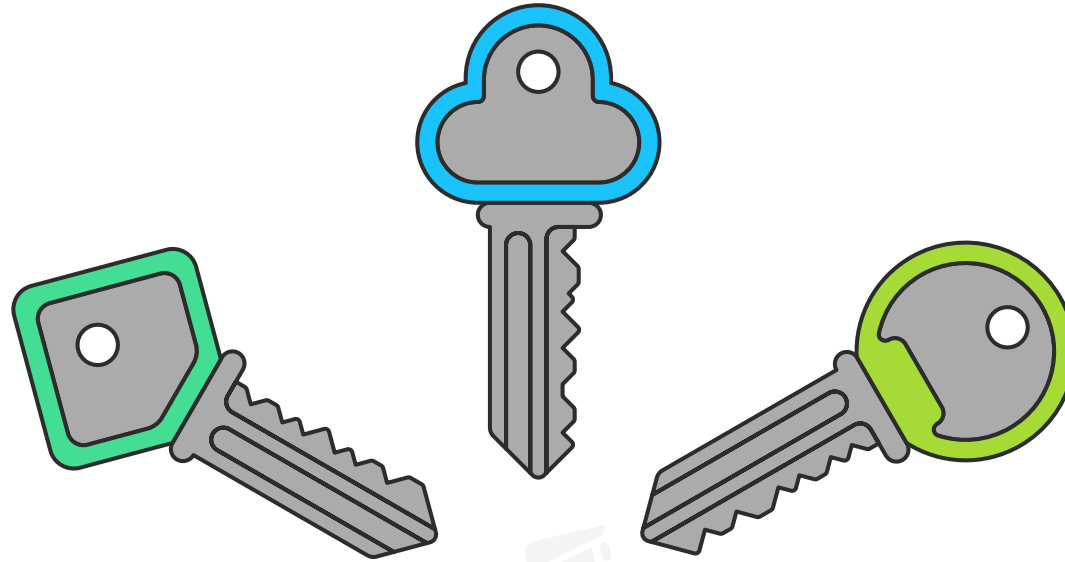


Building Human Resistance Behaviors

People, Process & Technology

Organizational
Readiness

AI Defense



Human
Resilience



AI Security Strategy



Technology: Email, Detection, Analytics



Process: Organizational Readiness



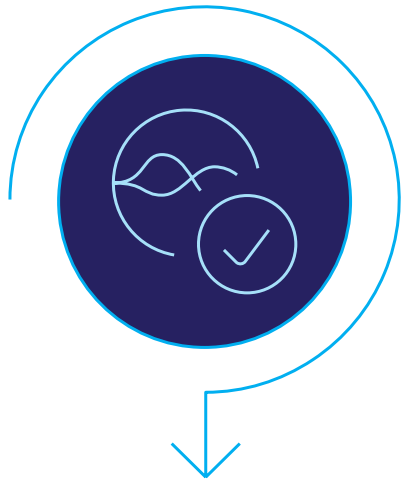
People: Before You Click, ask is this Expected?

Human Resilience – What Should We Be Asking?

~~Is this a deepfake?~~

**Train Users to Follow
Verification Procedures**

Layers of Detection



Verify

Confirm the media
content



Source

Consider the source
and determine
identity



Question

Challenge the validity
of the video / audio



Monitor

Observe media
streams for potential
deepfakes





Ongoing Security Awareness Behavior Change



What Happens Next?



The Leadership Deliverable



A Vigilant Human: That Stops the Attackers

Interested in Learning More?

<https://www.resemble.ai/deepfake-database/>

<https://www.aiaaic.org/aiaaic-repository>

<https://incidentdatabase.ai>

[Reality Defender AirTable](#)



AI Voice Generator Detect Resources

Government Pricing Sign In

AI Safety

Deepfake Incident Database

A curated database tracking verified incidents where deepfake technology has been used to target specific individuals or organizations. This collection documents cases of AI-generated synthetic media being weaponized for impersonation, manipulation, or deception, and its potential impact.



AIAAIC Repository

The independent, open, public interest resource detailing incidents and controversies driven by and relating to AI, algorithms and automation. [More](#)

Latest entries

- Suno AI accused of violating "Mambo no.5" copyright
- ElevenLabs accused of recreating French dubbing artist's voice
- The Brutalist AI voice cloning sparks jobs controversy
- Never used for using broadcaster content to train AI systems



AI Incident Database

Welcome to the AI Incident Database

Search over 3000 reports of AI harms

Reality Defender Deepfake News

News (2025) Facts and Figures Legislation Tracker Notable Deepfake Incidents News (2024) News (2023) External Resources (WIP) Reality Defender in the News

Views Grid view 50 Hide fields Filter Group IT Sorted by 1 field

	Target	Role/Title	Industry/Field	Reported Incident	Use Case	Quantifiable Impact	Date
1	Gisele Bündchen and other celebrities	Supermodel	Consumer products (s...)	Scammers in Brazil used ...		More than 20 million reais...	10/5/2025
2	Online consumers in Brazil	Consumers	Consumer	Brazilian consumers were...		More than 20 million reais...	10/5/2025
3	Ladakh Director General of Police (DGP) S.D. ...	Ladakh Director General ...	Law Enforcement	A deepfake video falsely ...		N/A	10/3/2025
4	Martin Wolf	Financial Times columnist	Media	Financial Times columnist...		N/A	10/2/2025
5	Donald Trump	President of the United St...	Healthcare/Wellness P...	Donald Trump posted an ...		N/A	9/30/2025
6	Democrats	Senate Minority Leader	Politics	Donald Trump posted an ...		N/A	9/30/2025
7	Sonam Wangchuk	climate activist	Government/Public Se...	A deepfake video falsely ...		N/A	9/30/2025
8	A group of longtime friends in Minnesota	Minnesota women (group...	N/A	A group of Minnesota wo...		N/A	9/28/2025
9	President Anura Kumara Dissanayake	President of Sri Lanka	Financial services / Cr...	A deepfake video falsely ...		N/A	9/28/2025
10	MGM China investors	Co-chairperson and exec...	Gambling/Casino	MGM China warned the p...		N/A	9/27/2025
11	Pope Leo XIV	Pope	Religion	The Vatican has been str...		N/A	9/26/2025
12	Francis J. Kong	Inspirational Speaker	Motivational Speaking	A false AI-generated ima...		N/A	9/26/2025
13	Mike Rowe	N/A	N/A	N/A		N/A	9/25/2025
14	Fans of Rafael Nadal	Recently retired tennis ch...	Financial services	Rafael Nadal was imperso...		N/A	9/25/2025
15	Bill Belichick and Jordon Hudson	college football coach an...	Sports	A fake AI-generated vide...		N/A	9/23/2025

3 Things To Do Next

1. Take the Extra Moment
2. Trust the Process, not the voice
3. If something feels off, say something

Thank You



Scan this QR code



Or go to

<https://talk.ac/jamesmcquiggan>

and enter this code when prompted

TALK

James R. McQuiggan | Apparent Security