Test Intro Video / Audio

This presentation may contain simulated phishing attacks.

The trade names/trademarks of third parties used in this presentation are solely for illustrative and educational purposes.

The marks are property of their respective owners, and the use or display of the marks does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4.

Cybercriminals don't care about this and use them anyway to trick you….

KnowBe4

Charlotte ISSA
Information Systems Security Association

Deepfakes & Art of Deception

Understanding Deepfakes with a hands-on approach

James R. McQuiggan, CISSP, SACP
Security Awareness Advocate


JEN EASTERLY
Ooastor, CbiA

James R. McQuiggan
CISSP, SACP, OSC

Security Awareness Advocate, KnowBe4 Inc.

Professor, Cyber Threat Intelligence, Full Sail

ISC2 North American Advisory Council

Past President, ISC2 Central Florida Chapter

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa

CISSP Certified Information Systems Security Professional
ISC2 Certification

H LAYER CREDENTIALING
CERTIFIED
Security Awareness and Culture Professional (SACP)

OSC
OPEN-SOURCE
CERTIFIED

About KnowBe4

We help over 70,000 organizations build a strong security culture to manage the ongoing problem of social engineering and human risk.

Top 100 Global Software Companies BEST SOFTWARE AWARDS 2024

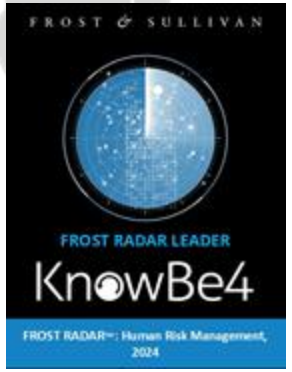
Trusted by 47 of the world's top 50 cybersecurity companies, and the largest human risk management platform

Gartner Magic Quadrant Leader

Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide

TrustRadius Top Rated 2024

CEO, leadership and Knowsters are industry veterans in cybersecurity



Office in the USA, UK, Canada, France, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Empowering your workforce to make smarter security decisions every day.


SECURITY
AWARENESS

Workshop Agenda

This Is Not the CEO You're Looking For: A Hands-On Deepfake Defense Workshop

Hour 1

- Introduction to Deepfakes
- Current Attack Vectors
  - Demo

Hour 2

- OSINT to gather info on mark
- Audio Cloning tools
- hands-on
- Show & Tell

Hour 3

- Video Cloning Tools
- hands-on
- Show & Tell

Hour 4

- Detection Tools
- Human Risk for Deepfakes Detection

Outcomes for Today

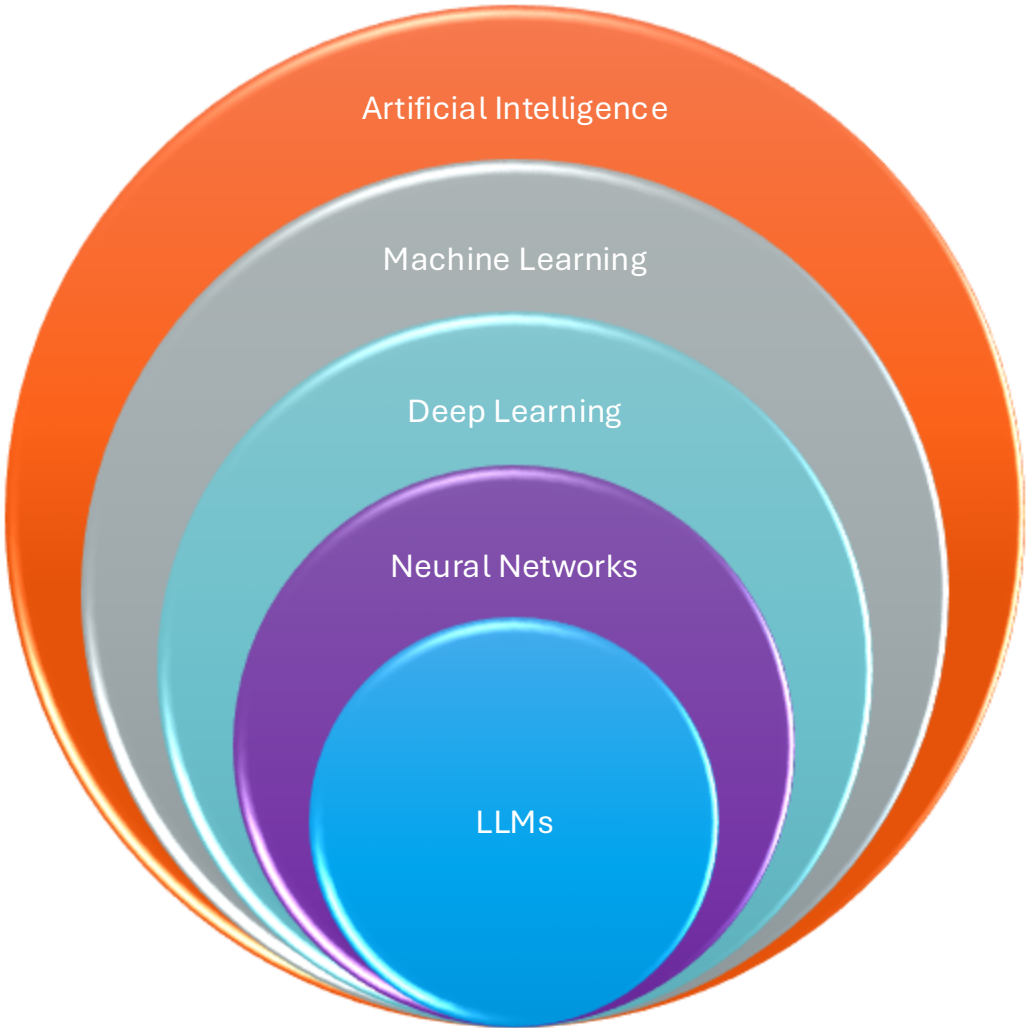
Train users to detect visual and audio deepfakes

Create simulation environments for social engineering scenarios

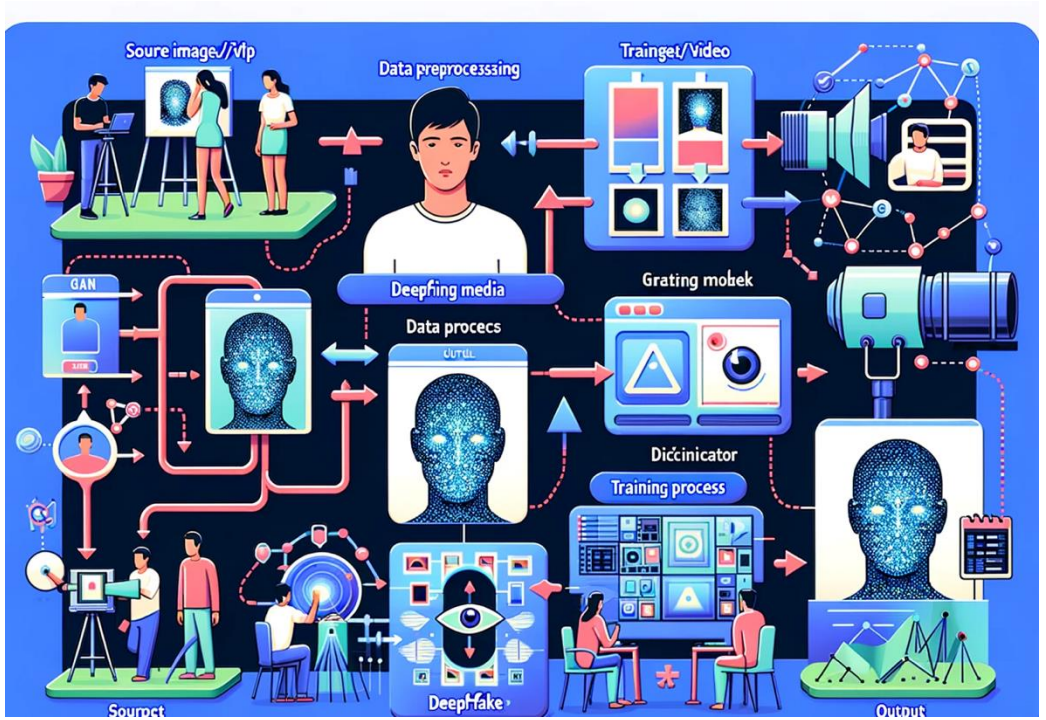
Demonstrate impersonation risks in live settings

Raise awareness on identity spoofing and trust indicators

Artificial Intelligence, Deepfakes, Synthetic Media

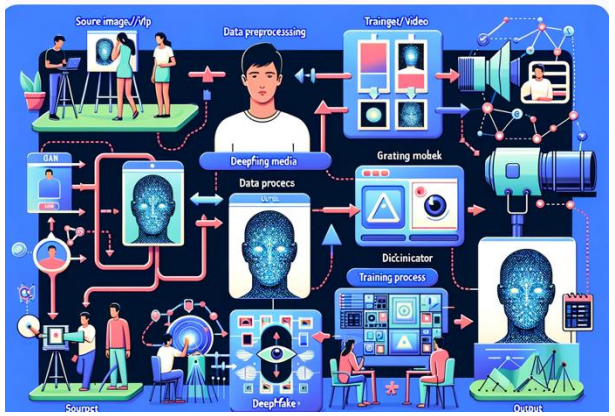


GAN Models



Generative Adversarial Models

GAN Models



Fools the discriminator

Identifies fakes

Creates synthetic data

Evaluates data realism

Generator

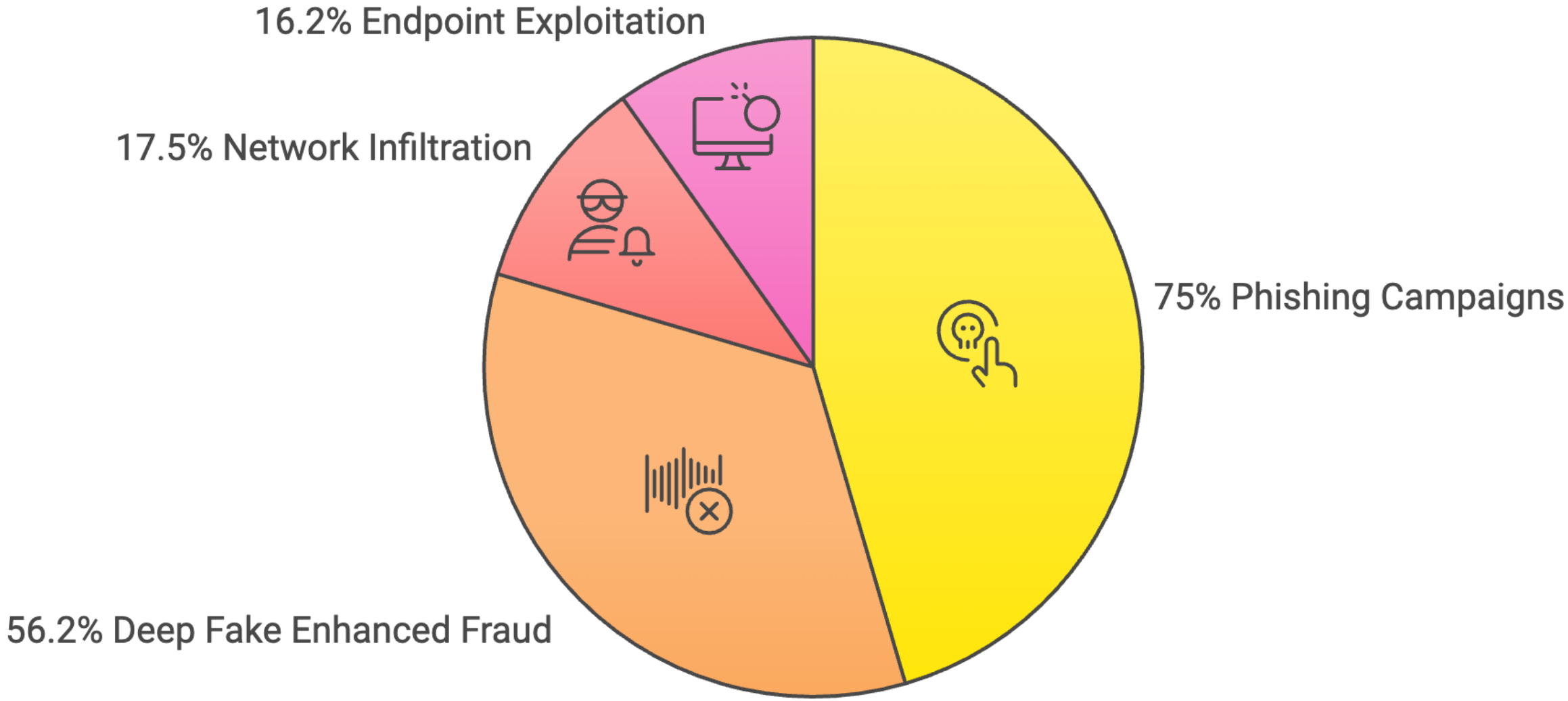
Discriminator

inator

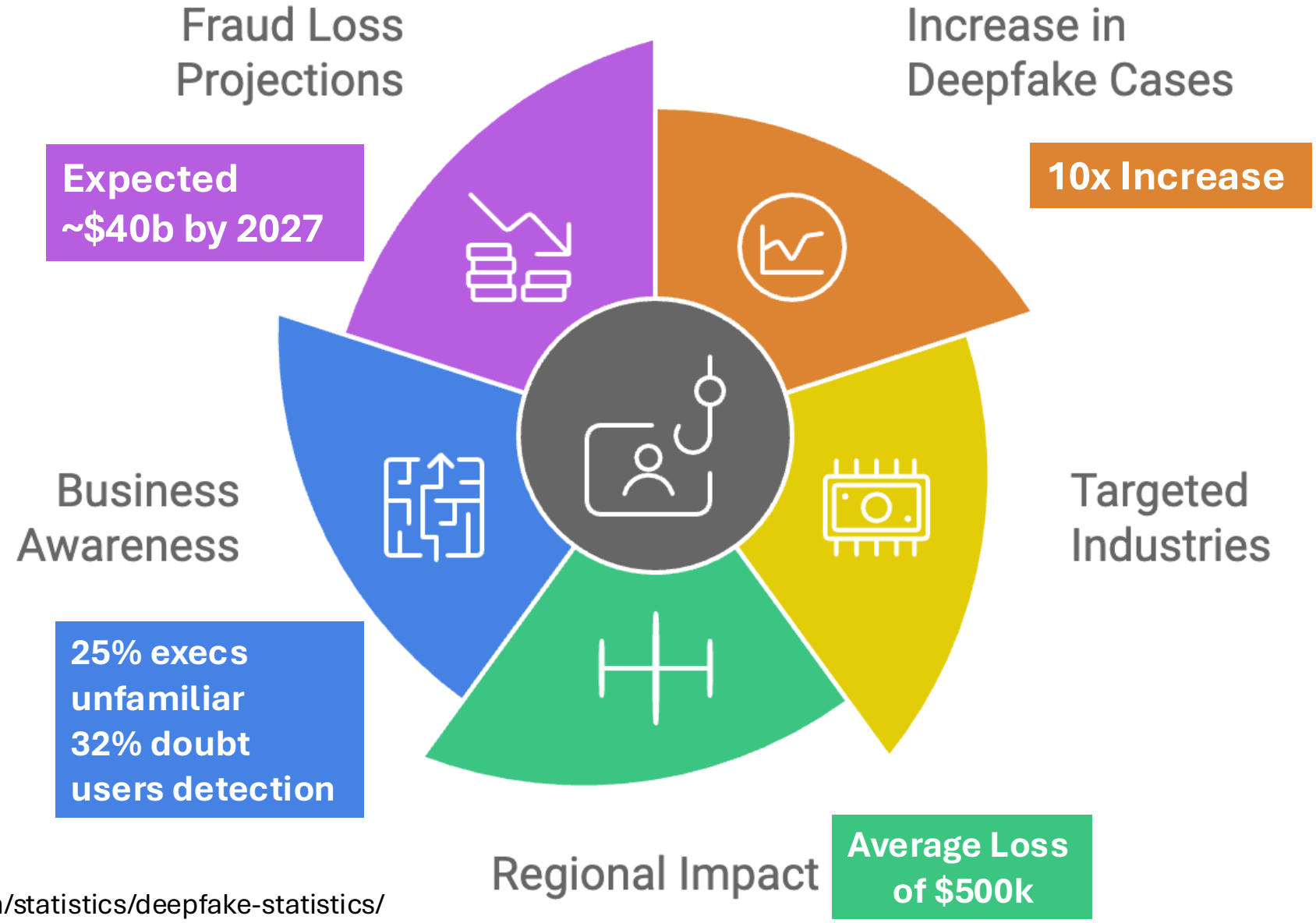
a authenticity

Roles and Goals of GAN Components

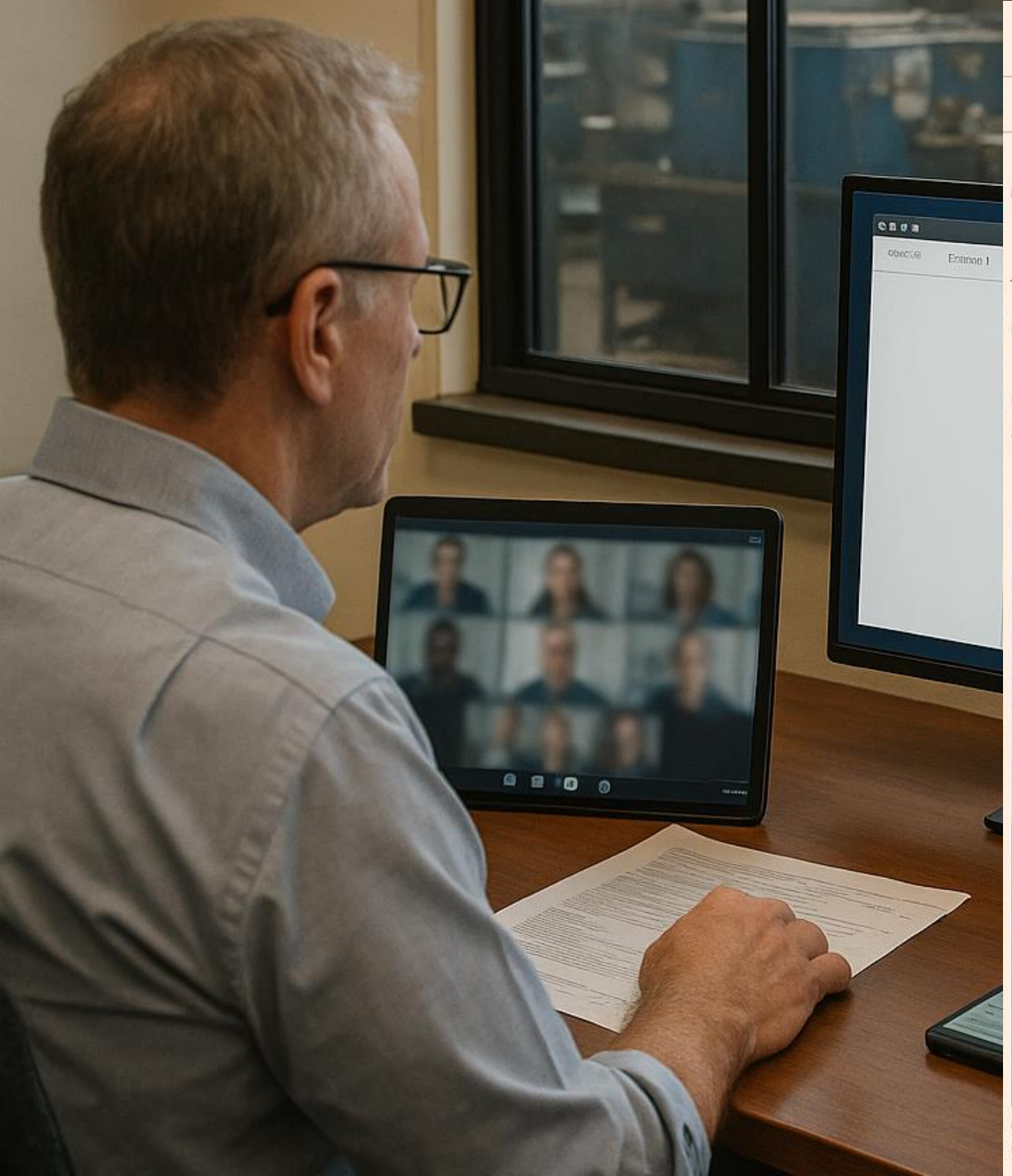
CISO Survey – AI Threats – Team 8



Deepfake Threats



Source: https://eftsure.com/statistics/deepfake-statistics/



COMPANIES TECH MARKETS

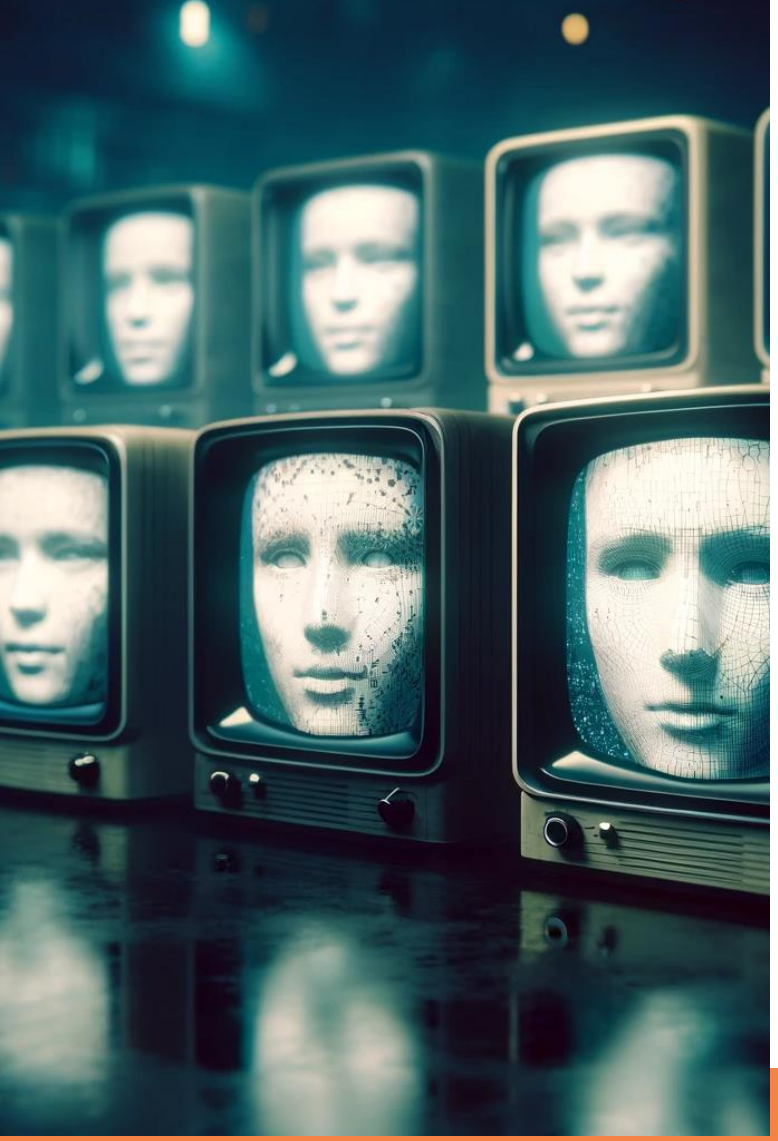
Cyber Security + Add to n

Arup lost $2 conference s

UK-based engineering g trick staff

Companies are at growing risk fro
© Getty Images


“A” AI Playbook for Cybercriminals
Synthetic Media / Identities
Zero Click Worm (GenAI)
RAG Exploits
ASCII Attacks
Hallucinations / Biases
Polymorphic Malware
Automated Attacks
Password Cracking
Data Poisoning
Prompt Injection
Malicious AI LLMs
AI Phishing / Spear Phishing
Agentic AI Attacks
Shadow AI



Synthetic Media

Synthetic Text

Microsoft Copilot

Gemini

Claude

n Sport Culture Lifestyle

US

The Guardian

a Australia Middle East Africa Inequality Global development

Australian lawyer caught using ChatGPT filed court documents referencing 'non-existent' cases

Immigration minister says such conduct must be 'nipped in bud' as lawyer referred to office of the NSW Legal Services Commissioner for consideration

Malicious LLMs

Six-Month Phishing Snapshot

17.3%
increase in phishing emails (vs. previous six months)

Between Sep 15, 2024, and Feb 14, 2025

57.9%
were sent from compromised accounts

11.4%
within the supply chain

25.9%
contained attachments

20%
relied solely on social engineering

54.9%
contained a phishing hyperlink payload

Six-Month Phishing Snapshot

57.9%
were sent from compromised accounts

25.9%
contained attachments

11.4%
within the supply chain

20%
relied solely on social engineering

54.9%
contained a phishing hyperlink payload

Six-Month Phishing Snapshot

17.3%
increase in phishing emails (vs. previous six months)

Between Sep 15, 2024, and Feb 14, 2025

57.9%
were sent from compromised accounts

11.4%
within the supply chain

25.9%
contained attachments

20%
relied solely on social engineering

54.9%
contained a phishing hyperlink payload

Six-Month Phishing Snapshot

17.3%
increase in phishing emails (vs. previous six months)

Between Sep 15, 2024, and Feb 14, 2025

57.9%
were sent from compromised accounts

11.4%
within the supply chain

25.9%
contained attachments

20%
relied solely on social engineering

54.9%
contained a phishing hyperlink payload

Polymorphic Phishing

Evasion by design

Key elements mutate on every send.

Bypassing legacy tools

Signature-matching fails because variants differ.

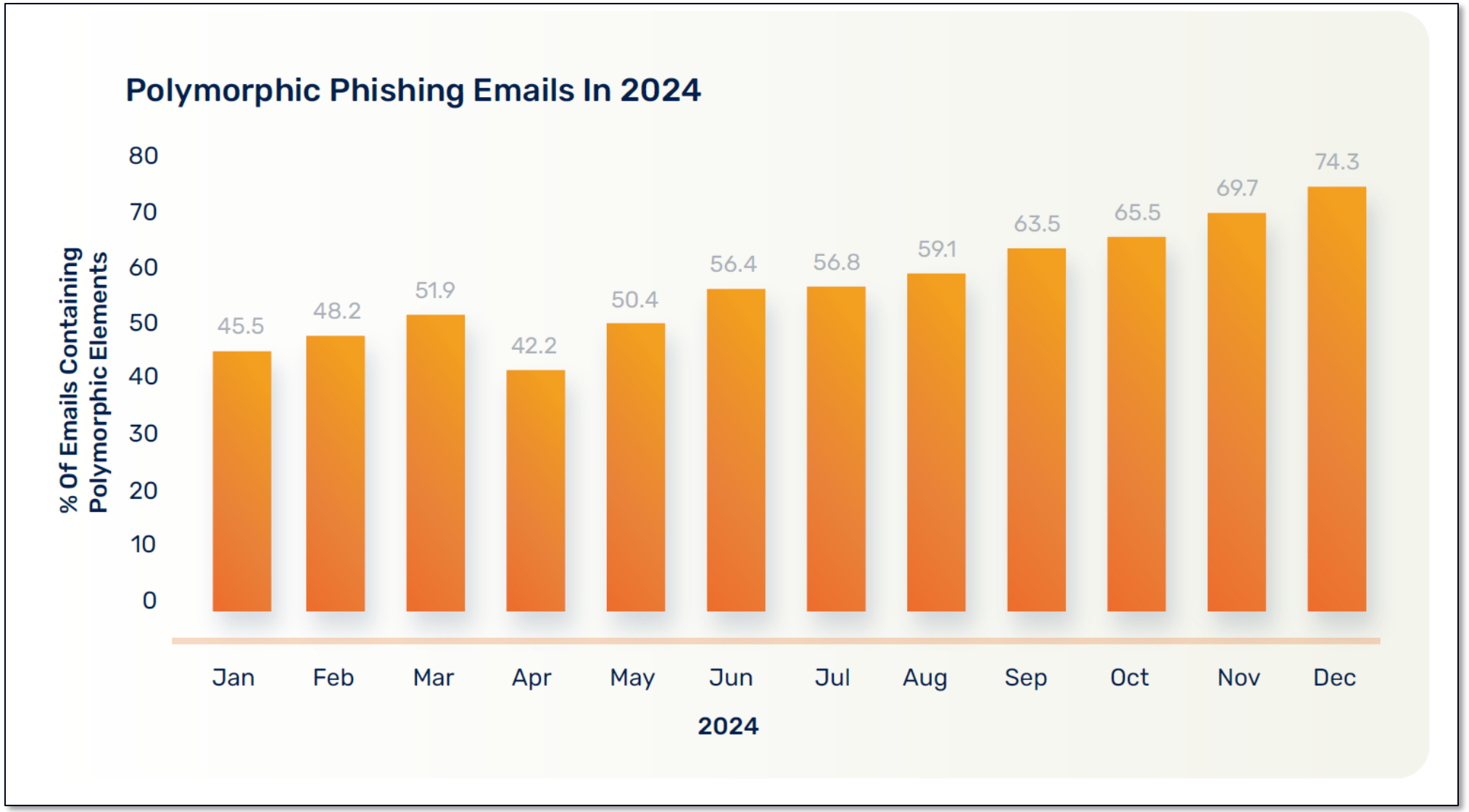
Scalability via AI

LLMs mass-produce varied phishing emails.

Dynamic payloads

Email content morphs based on user.

Polymorphic Emails



Synthetic Images

Synthetic Images - Deepfakes

BRAD PITT

AI scammers pretending to be Brad Pitt con woman out of $850,000

Pitt does not have any verified social media platforms

NEWS › FILM NEWS

Brad Pitt fraudster scams French woman out of $800,000 using AI

"He knew how to talk to women and it was very well put together"

French woman says she was conned out of $850,000 by an AI Brad Pitt

The woman chatted with the AI Pitt for more than a year and sent the scammer money to help with a fake kidney treatment

Viral scam: French woman duped by AI Brad Pitt love scheme faces cyberbullying


HOLLYWOODD
GROK

Synthetic Audio

Synthetic Audio and Social Engineering

LASTPASS LABS

Attempted Audio Deepfake Call Targets LastPass Employee

Mike Kosak • April 10, 2024

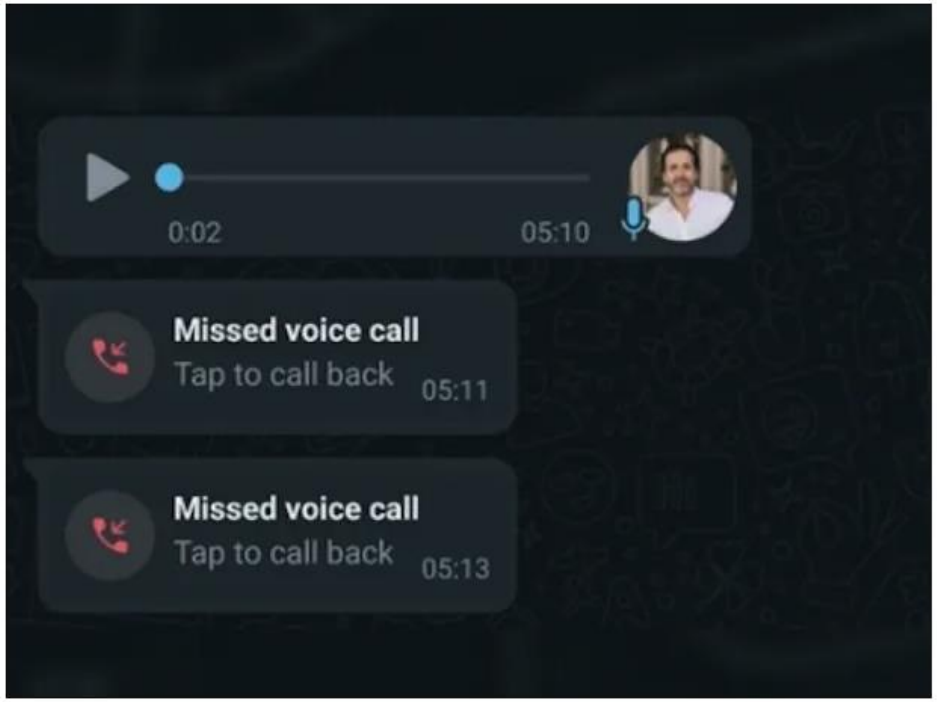
Mike Kosak, Senior Principal Intelligence Analyst at LastPass, explained in a blog post, "In our case, an employee received a series of calls, texts, and at least one voicemail featuring an audio deepfake from a threat actor impersonating our CEO via WhatsApp.

Audio Deepfake Attacks: Widespread And 'Only Going To Get Worse'

BY KYLE ALSPACH

OCTOBER 3, 2024, 11:23 AM EDT

A cybersecurity researcher tells CRN that his own family was recently targeted with a convincing voice-clone scam.



Using Questions / Be Curious

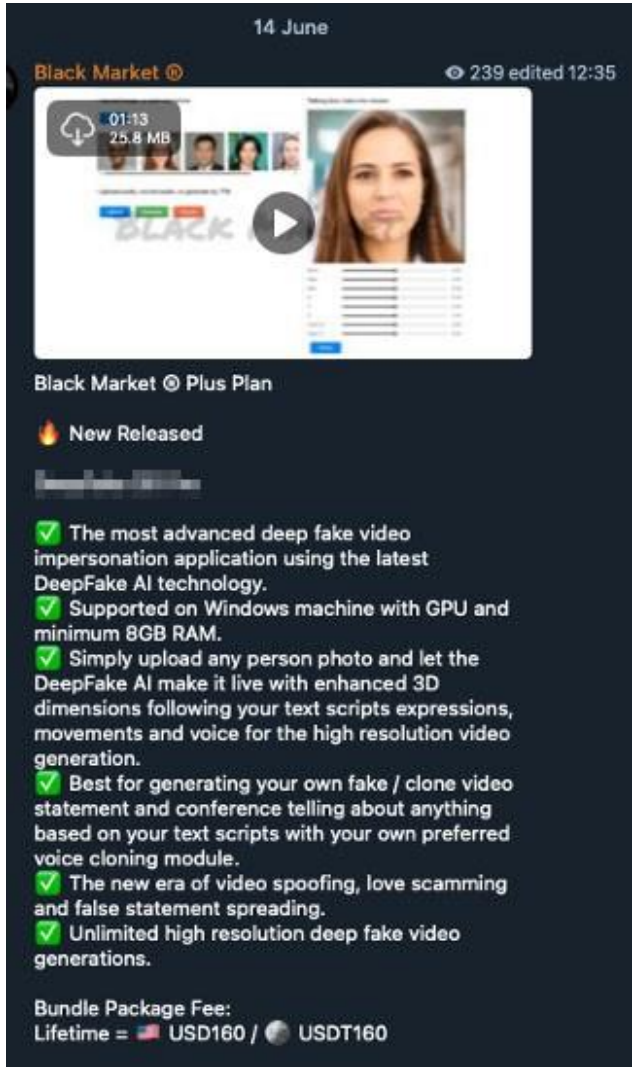
"What is the book that you recommended to me?"

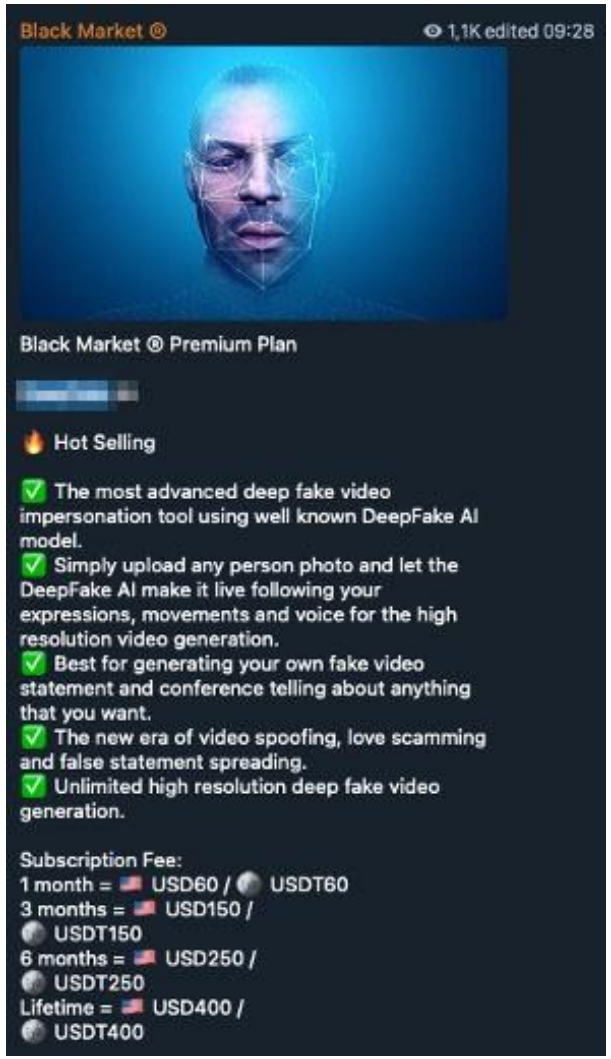
FlipSide – Used Against the Scammers

AI vs AI

Synthetic Video

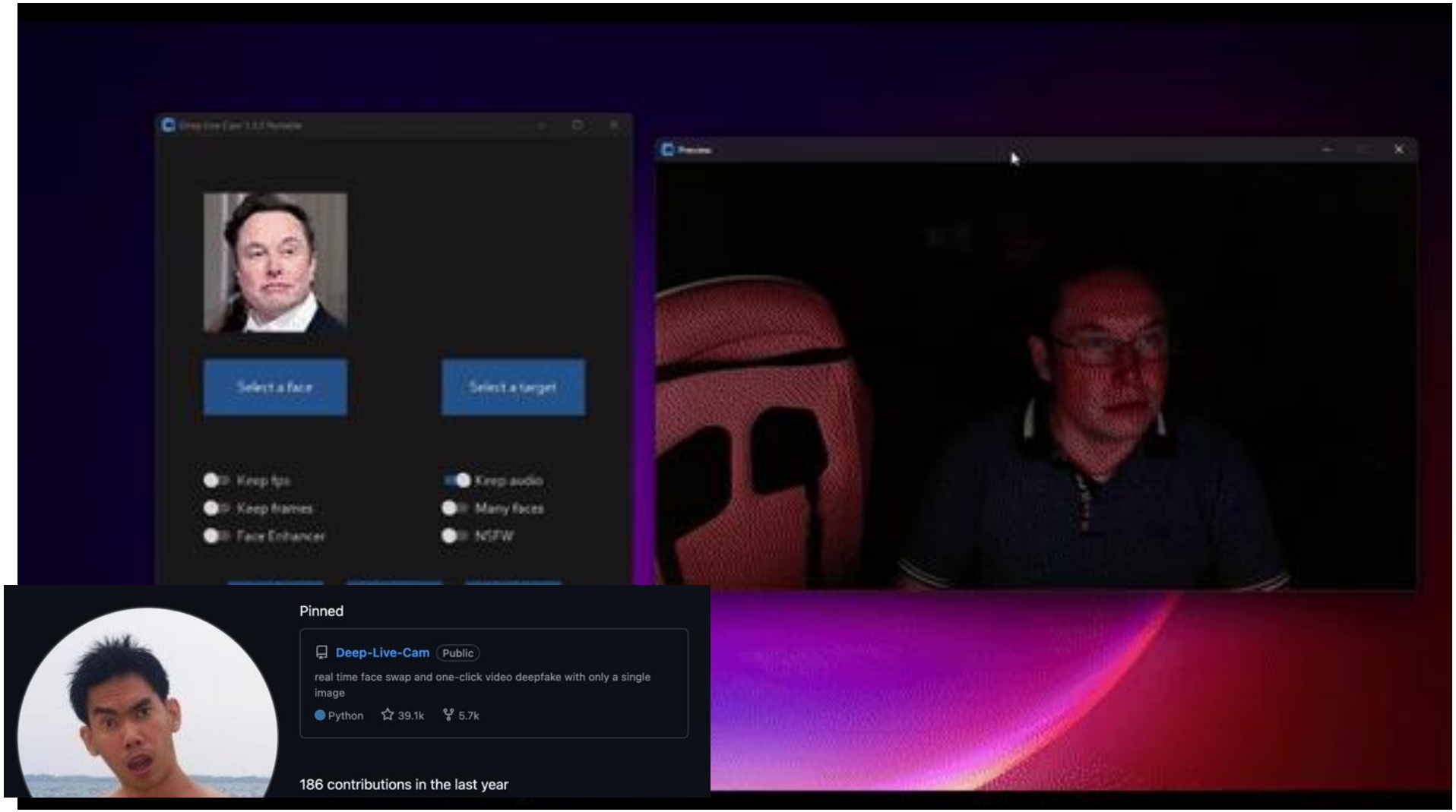
Dark Web Activity





Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/surging-hype-an-update-on-the-rising-abuse-of-genai

Face Swap / Voice Cloning & Webcams -> LIVE Deepfakes



Tool List

For detailed instructions please refer to the websites or GitHub pages of the individual tools.

Deep Face Lab is a program for training deepfake models and using them to make pre-recorded videos. Its GitHub page has been taken down, but you can still find a detailed guide for it here.

Deep Face Live uses models trained with Deep Face Lab to make real time deepfakes. It comes with several pre-made models and its GitHub page can be found here.

Live Portrait is a tool for copying facial expressions from a source video onto a target image or video. Its GitHub page can be found here.

Ollama is a framework for locally hosted LLMS which are capable of uncensored text generation. Read more about it here.

RVC is an open source tool for voice cloning with a web interface. Its GitHub page is available here.

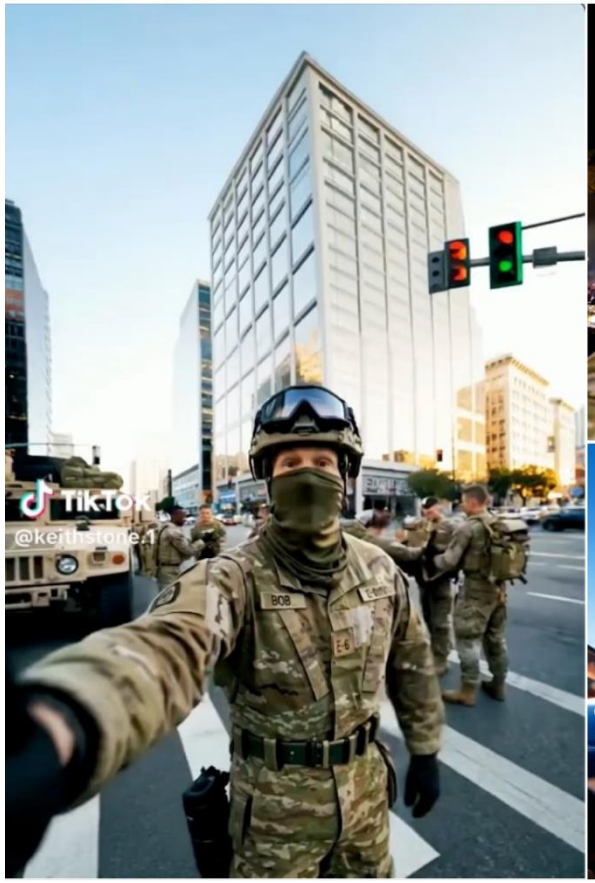
Disinformation Campaigns

The National Guard's post

The National Guard
5d ·

Several videos from "Bob" have been making the rounds online. They are fake. Red flags indicating a fake: The uniform name tape reads "Bob," his rank reads "E-6," and there is gibberish where "U.S. Army" should appear. In one video, the AI-generated "man" even eats a burrito through a mask.

https://www.nationalguard.mil/.../guard-identifies-ai...



Hany Farid · Following
UC Berkeley Professor & GetReal Co-founder
14h · Edited ·

In just the last 12 hours, we at GetReal have been seeing a slew of fake videos surrounding the recent conflict between Israel and Iran. We have been able to link each of these visually compelling videos to Veo 3.

It is no surprise that as generative-AI tools continue to improve in photo-realism, they are being misused to spread misinformation and sow confusion.

One simple tip-off (for now at least) is that all of these videos are either exactly eight seconds in length or composed of short (eights seconds or less) clips composited together. Why eight seconds? This is the current maximum length that Veo 3 can generate a continuous shot. Other models have slightly longer limits but 8-10 seconds is typical.

This eight-second limit obviously doesn't prove a video is fake but should be a good reason to give you pause and fact-check before you re-share.

You and 362 others

21 comments · 51 reposts

Generative AI Dangers – Survey of Concerns & Potential Problems

AI Scams — 71%

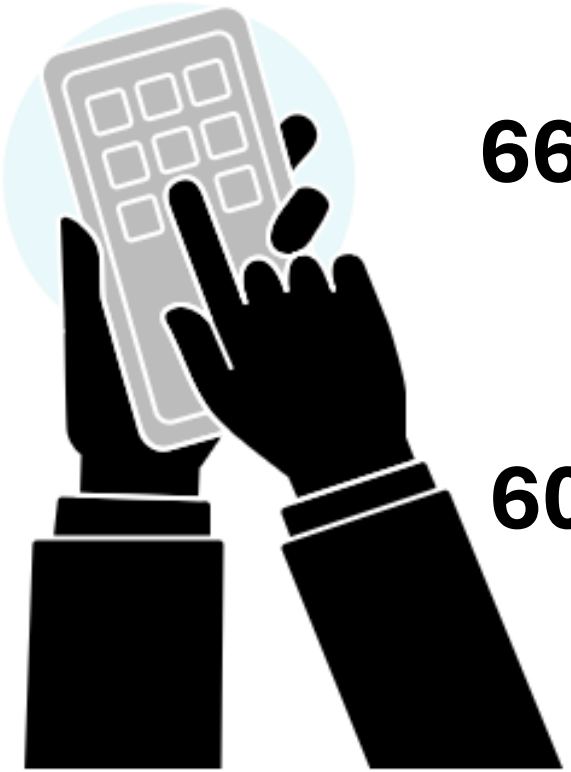
Scams perpetrated using artificial intelligence technologies.

Sextortion — 69%

Online blackmail involving sexual images or videos.

Data Privacy — 62%

Concerns surrounding the collection and use of data.



Deepfakes — 69%

Realistic but fake media created using AI.

AI Hallucinations — 66%

AI generates false or misleading information confidently.

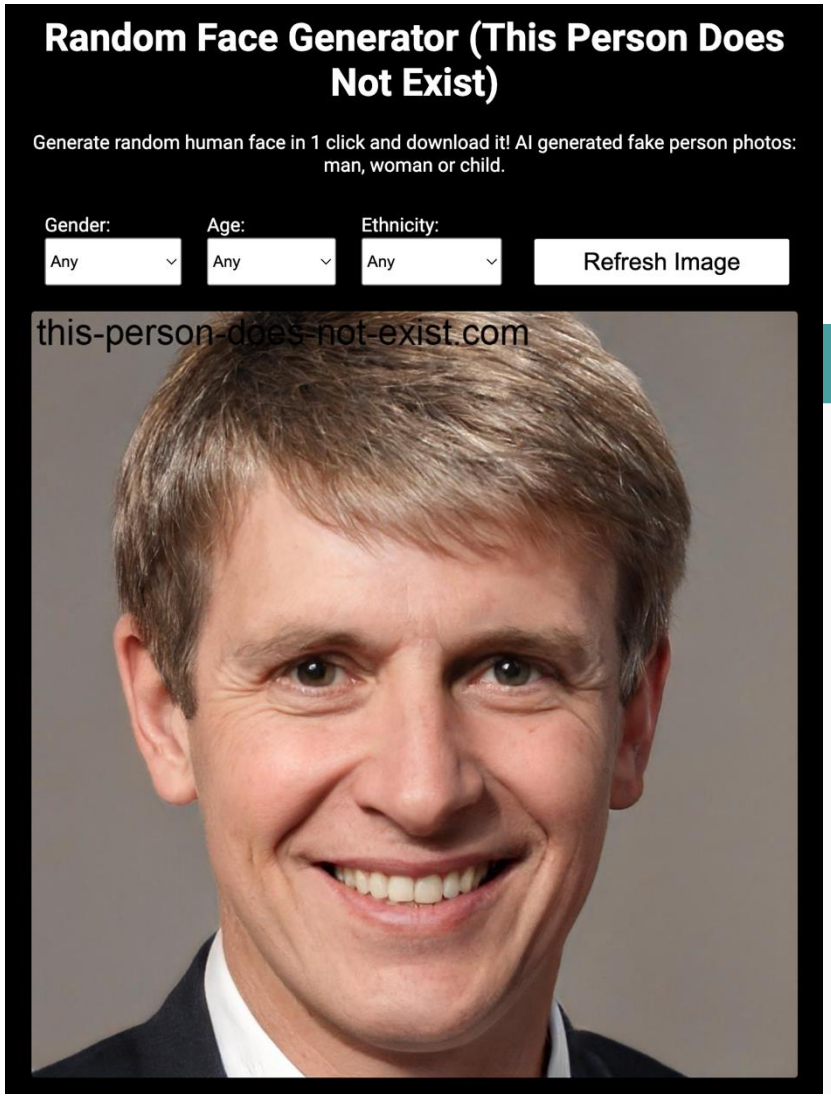
Bias Amplification — 60%

AI systems reinforce existing societal biases.

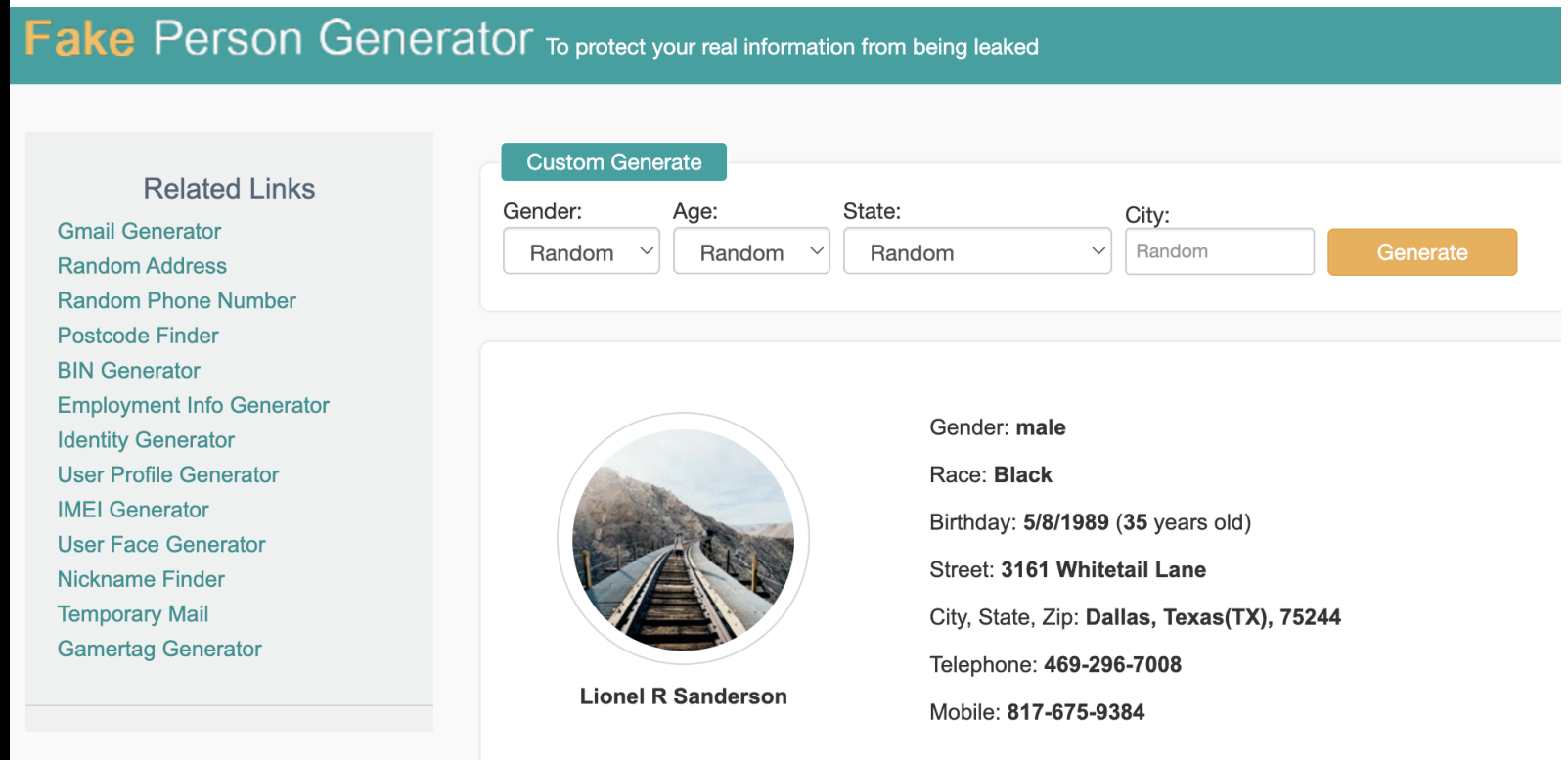
Source: Microsoft Global Onine Safety Survey 2024

Synthetic Identies

Synthetic Identities – Sock Puppet Accounts

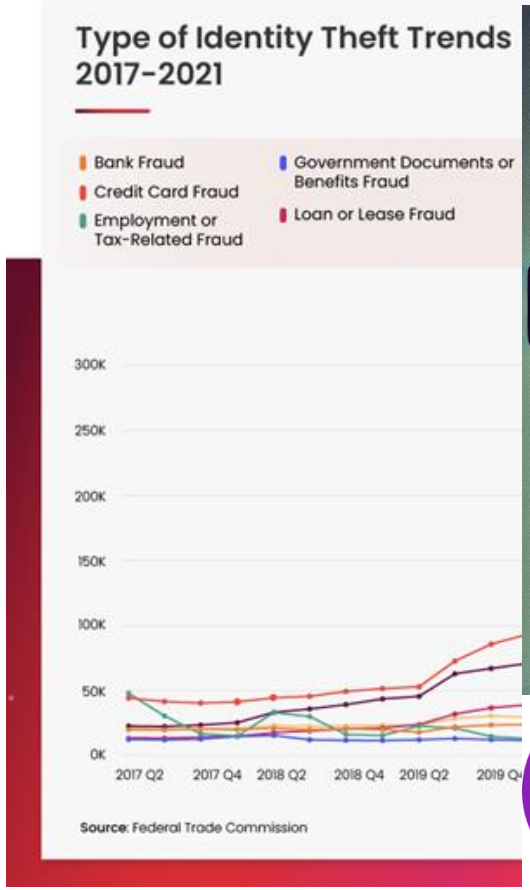


https://this-person-does-not-exist.com



https://www.fakepersongenerator.com

Synthetic Identity



Explosive Growth
Synthetic identity fraud cases surged 18% in 2024, making it the fastest-growing type of fraud.

Emerging Tactics
Face swaps and injection attacks increased by 704% in H2 vs H1 2023.

REWARD UP TO $5 MILLION FOR INFORMATION ON NORTH KOREAN IT COMPANIES, WORKERS & RELATED MONEY LAUNDERING

IT firms Yanbian Silverstar, based in the People's Republic of China (PRC), and Volasys Silverstar, based in Russia, generate revenue by deceiving U.S. and other businesses worldwide into hiring their North Korean staff as freelance IT workers. The companies then launder their ill-gotten gains to North Korea, in violation of U.S. and UN sanctions.

We are seeking information on Yanbian and Volasys Silverstar-linked individuals who help to generate illicit funds for the North Korean regime.

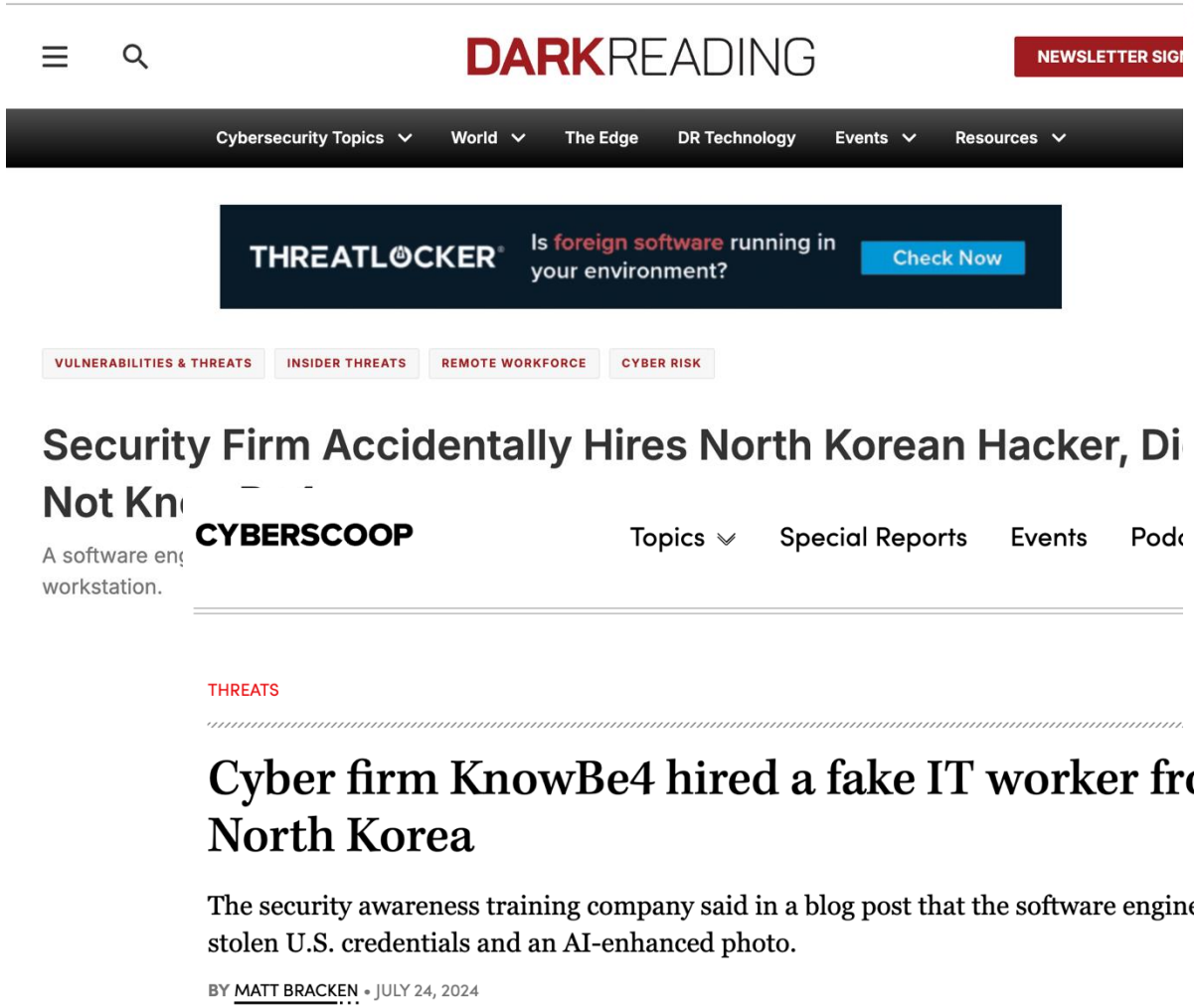
If you have information on these individuals, their activities, or associated persons or entities, contact us via our Tor-based tip line below. You could be eligible for a reward and relocation.

Tor Link: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion

U.S. Department of State
Diplomatic Security Service
Rewards for Justice

+1-202-702-7843
@RFJ_USA

KnowBe4 In The Headlines...



We Blogged About It...

X Post Button

23 Jul

How a North Korean Fake IT Worker Tried to Infiltrate Us

Stu

25 Jul

North Korean Fake IT Worker FAQ

Stu

27 Jul

How The Whole World Now Knows About Fake North Korean IT Workers

Stu Sjouwerman

Post Share Share 5

Wow! Last week's blog post went viral, reaching major media outlets and receiving over 125,000 views within days. Responses from around the world praised our transparency and commitment for doing what's right, though some had negative reactions.

I decided to write an FAQ with more detail and reiterate that this was not a data breach but rather a public service announcement: https://blog.knowbe4.com/north-korean-fake-it-worker-faq

KnowBe4 & The North Korean Employee

Application Submission

Fake identity applied for a job

NK Hiring Evidence

Kyle David Parkhurst

Senior Software Engineer

[redacted]gmail.com (404) [redacted] Atlanta, Georgia, US LinkedIn

SUMMARY

I am a seasoned senior software engineer with over 12 years of comprehensive experience in developing scalable and efficient digital solutions across various platforms. Passionate about leveraging my extensive experience in software engineering, I focus on developing robust and scalable systems, employing the latest technologies to solve complex challenges and enhance the user experience.

PROFESSIONAL EXPERIENCE

[redacted] May 2019 – April 2024

Senior Software Engineer

- Worked in the E-commerce division of the [redacted] engineering team, developing a membership management portal for over 1M active users with a focus on performance using React, Vue.js, Redux, Typescript, Node.js and AWS, in a professional Agile environment.
- Built a reusable and highly customizable component library used across 12 engineering teams, leveraging Storybook for robust development.
- Utilized Express middleware to efficiently query a GraphQL endpoint, leveraging middleware functions for routing and error handling, which streamlined development and improved data retrieval performance.
- Leveraged AWS services, including AWS Lambda, API Gateway, CloudFront, and Amplify, to architect and develop scalable and secure serverless applications, resulting in cost optimization and enhanced application performance.
- Mentored 2 junior developers and led technical sessions with team members to discuss trending technologies.
- Performed detailed code reviews with a team of 15 developers, enforcing coding standards to enhance code quality and promote adherence to best practices.

[redacted] January 2015 – April 2019

Full Stack Developer

- Played a key role at IT service portal modernization project, collaborating closely with multiple teams to conceptualize and develop software solutions using React, Redux Toolkit and Node.js.
- Implemented best practices in software development and architecture, ensuring that applications are compliant with industry standards.
- Worked with multiple business partners of [redacted] from different industries, utilized Node.js and Python to create and maintain RESTful and GraphQL APIs and Implemented and maintained high-quality, scalable user interfaces using React.js, and Vue.js.
- Developed and maintained automated testing suites using Jest, Enzyme, React Testing Library, Cypress, and Playwright, achieving over 95% test coverage and reducing bug rates by 40% across multiple projects.
- Improved product performance by 10% through effective optimization techniques such as code splitting and

Stock photo NK used

AI-Photo Blending NK

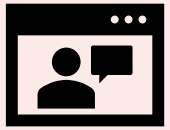
Real time Video Deep fake Face Swap – And It Continues…

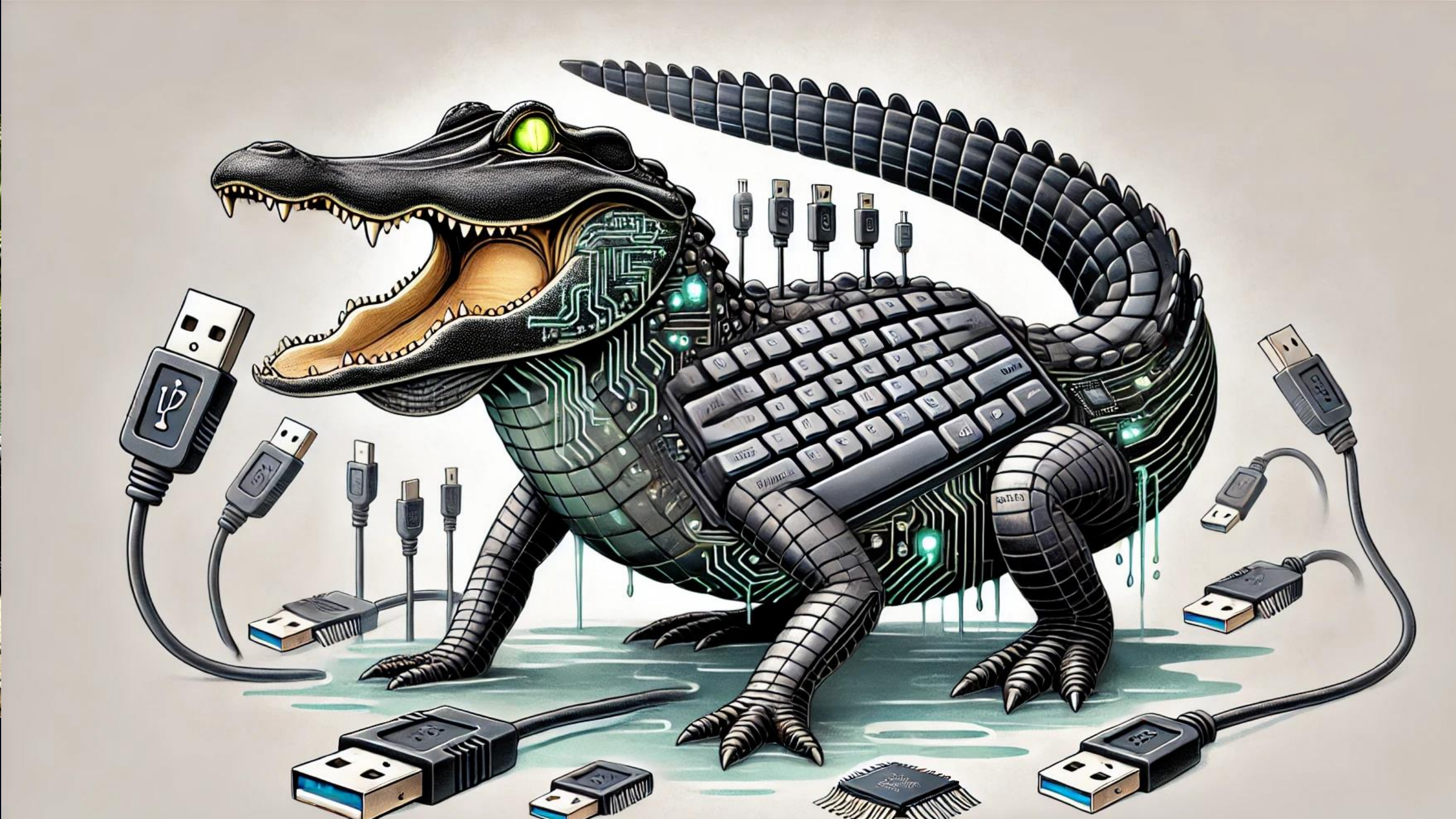
DOJ indicts two Americans for running laptop farm used in North Korea IT worker scam

The Justice Department indicted five people for their role in a scheme that allowed North Koreans to gain employment with at least 64 U.S. companies and earn hundreds of thousands of dollars for Pyongyang's government.

North Korean nationals Jin Sung-Il and Pak Jin-Song were indicted alongside Americans Erick Ntekereze Prince and Emanuel Ashtor as well as Mexican national Pedro Ernesto Alonso De Los Reyes.

Where Deepfakes Hit You Hardest: Threat Matrix

	Executive Leadership	Employees/ Internal Comms	External Stakeholders
	CEO Voice / Wire Fraud	IT Support call scams	Vendor Negotiation spoof
	Deepfake investor	HR termination hoax	Fake public statements
	Fake exec resumes	Impersonated colleagues	Fraudulent customer support

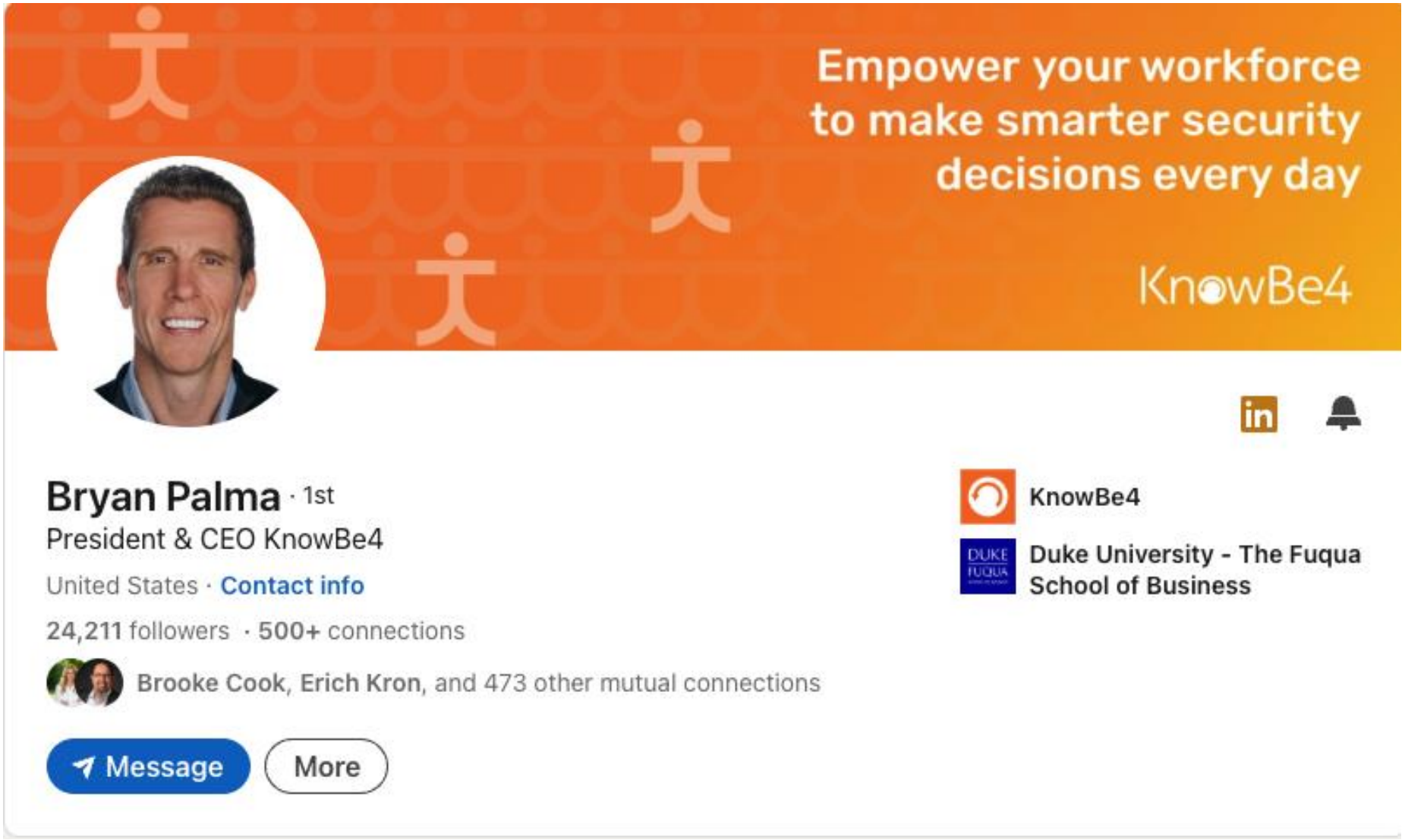



edge
BRAVE

BREAK – 10 minutes

DEMO – Soup to Nuts

My Target – Brian Palma



OSINT Tools – Investigation of Your Mark

- Google Dorks
- LinkedIn
- FaceCheck.ID
- Fast People Search

- YouTube
- Podcasts
- Conference Recordings

- Audio / Video recording of mark
- Headshot / clear, not pixelated

- At least 30 seconds
- Uninterrupted
- Just them talking
- Presentations, Podcasts

Audio Cloning

ChatGPT + Syn. Audio + Call Center = AI Social Engineering

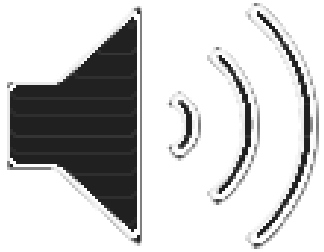
ChatGPT3.5 Prompt:

You are calling to tell me that you have been in a car accident and now he's being held by the police. Convince me that I need to send you $500 to pay the tow truck and start the repairs. You've been arrested and you don't have your wallet and you also need another $1500 to get you out of jail. The money needs to be sent as crypto currency as you know I have a crypto wallet and I can send money that way"

Using PlayHT

Dr. Gerald Auger, Simply Cyber (and friend)

Call Center
Support
Software



Audio Cloning / Deepfakes

- Download the Audio
  - YouTube Downloader
  - Airy
  - ytmp3.cc
  - colbalt.tools

- Audio Cleaning
  - Audacity / Audition / Descript
    - Cleaning audio
    - Adding audio

YT-DLP – Open Terminal / Command Prompt

- `yt-dlp -vF “https://www.youtube.com/watch?v=xxxxx”`
  - **Provides the codecs to download -> Look for mp3 / mp4 audio only**
- `yt-dlp -f yyy “https://www.youtube.com/watch?v=xxxxx”`
  - **Downloads the video format specified**
- `yt-dlp -x -audio-format mp3 “https://www.youtube.com/watch?v=xxxxx”` **– removes audio**
- `yt-dlp -f -download-sections “*00:00:45-00:01:15” -force-keyframes-at-cuts “https://www.youtube.com/watch?v=xxxxx”`
  - **Specific Timeframe**

Audio Cloning / Deepfakes

- Cloning Tools
  - ElevenLabs
  - PlayHT
  - Resemble

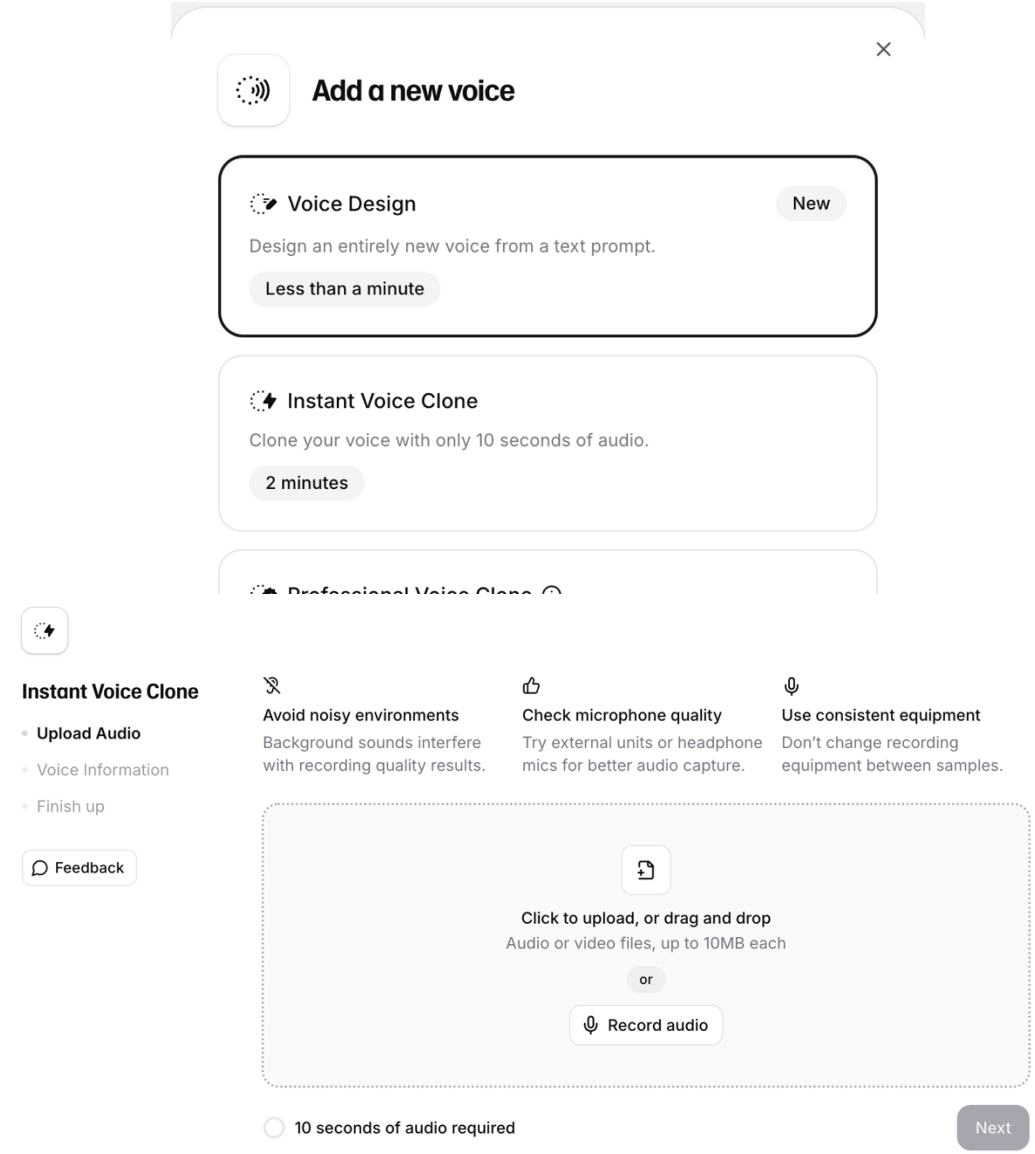
- LLM & Interactive Tools
  - Dialpad
  - VAPI

- Other Tools
  - Voicemod: Easy voice modulation with presets
  - Voice.ai: Real-time voice cloning from samples
  - RTVC: Open-source TTS-based voice synthesis
  - Altered.ai: High-quality voice transformations

ElevenLabs Instructions

- Sign in at elevenlabs.io
- Navigate to Voices in the sidebar
- Click Add a new voice
- Select Instant Cloning
  - upload 1–2 minutes of clean audio
- Upload the audio wav file to be trained
- Name your voice
- Save voice to your library
- Now Write the text you want it to say

Demo Video:
https://www.youtube.com/watch?v=8C5LVi5Keug



Video Cloning

Video Cloning – Image to Video

Image to Video

- Hedra
- LemonSlice
- Synthesia.io (if available)
- HeyGen
- Deepfake Offensive Toolkit (DOT)
- Akool

LipSyncing (Advanced)

- KlingAi – 8 to 10 seconds max
- Pixverse - https://app.pixverse.ai
- Synclabs - https://translate.synclabs.so/
- Akool – https://akool.com/apps/faceswap

Video Cloning – Image to Video

Realtime FaceSwap - Advanced

- DeepFaceLab
- Deep-Live-Cam
- SwapFace
- MagicCam

Key Features of Deepfake Tools

- Real-Time Face & Voice Swapping
- Virtual Webcam and Microphone Support
- Cross-Platform Compatibility
- Ease of Use vs Flexibility
- Educational Licensing Options
- Multi-avatar and Persona Capabilities

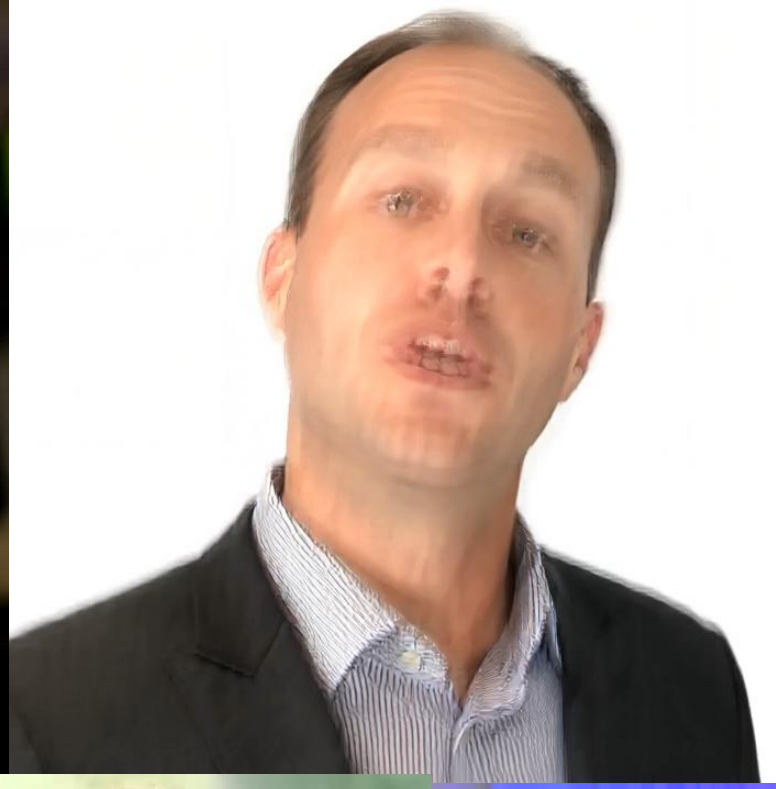
Commercial Tools Overview

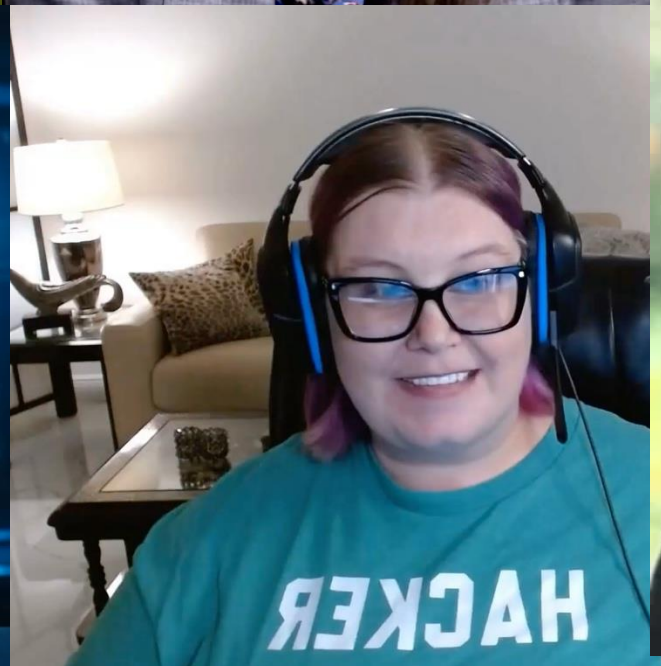
- Xpression Camera: Real-time facial transformation with ease
- Magicam (SwapFace): Full face and voice deepfake suite
- Snap Camera (Legacy): AR filters, no longer maintained
- Ideal for: Live demos, training scenarios, impersonation awareness


KnowBe4

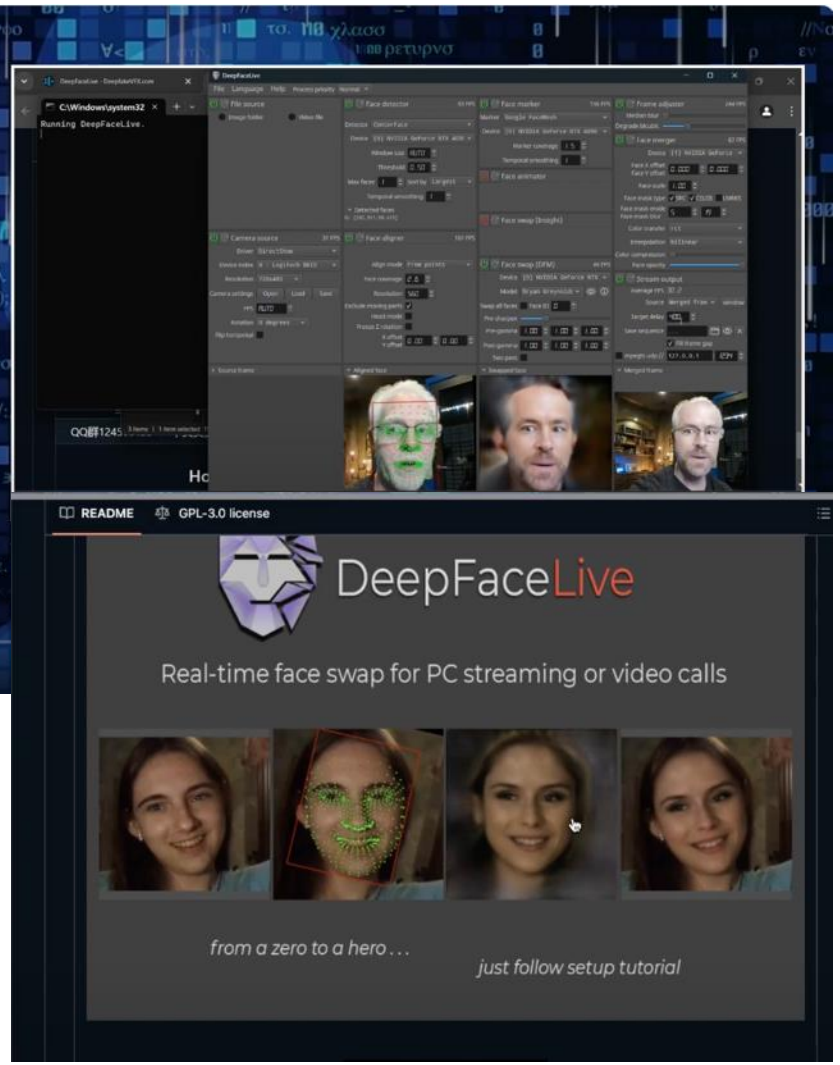

KnowBe4
Ahora podemos ir un paso más allá, ya que he creado mi propio Avatar






HACKER

Perry Carpenter – Deep Fakes



CREATE real-time DEEPFAKES (a.k.a. I became TAYLOR SWIFT...for Science!)

Source: https://www.youtube.com/watch?v=nKhtTIV6vxU


THE FAIK FILES
N2K


BOX

Live Faceswap Demo

BREAK – 10 minutes

Detection

Detection Tools

- Sensity AI
- Hive AI Deepfake Detection
- Microsoft Video Authenticator (if accessible)
- Deepware Scanner (Chrome Extension)

Online Quiz to Spot Deepfakes - https://spotdeepfakes.org/en-US/quiz

- Resemble
- Deepfake detector ai
- 11Labs
- Reality Defender

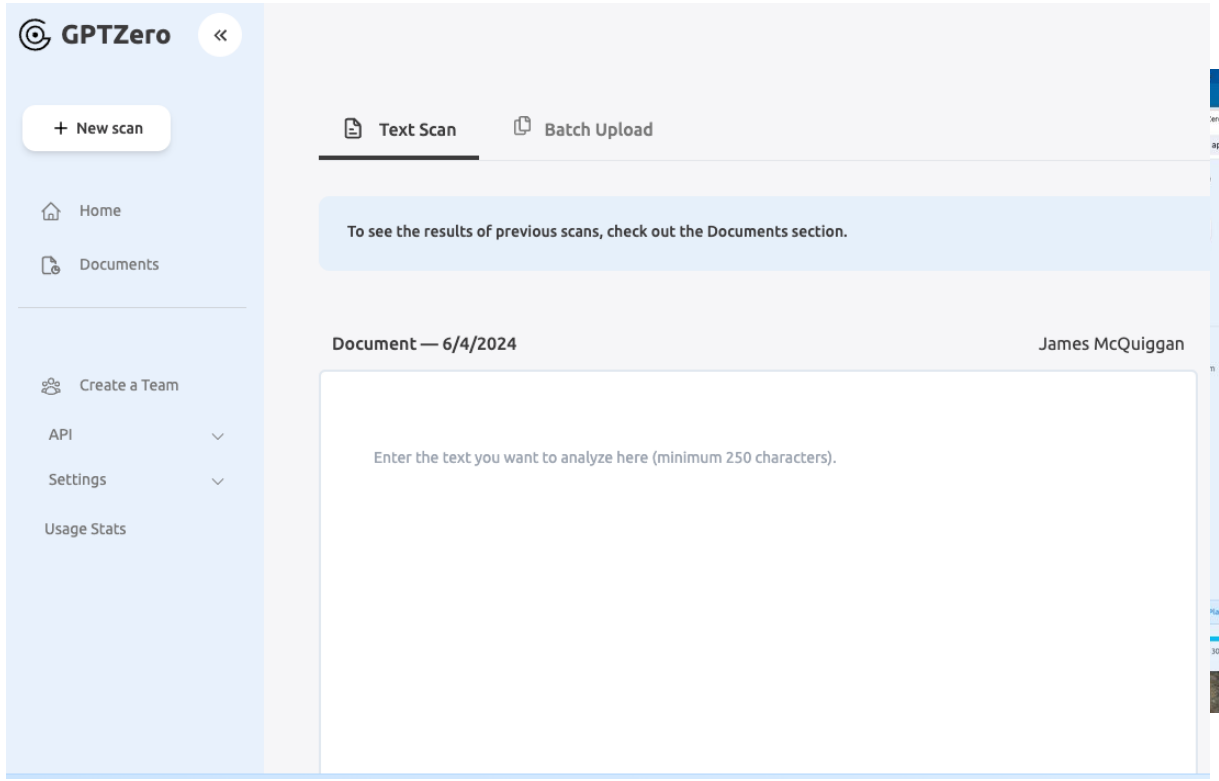
Advanced Techniques for Deepfakes

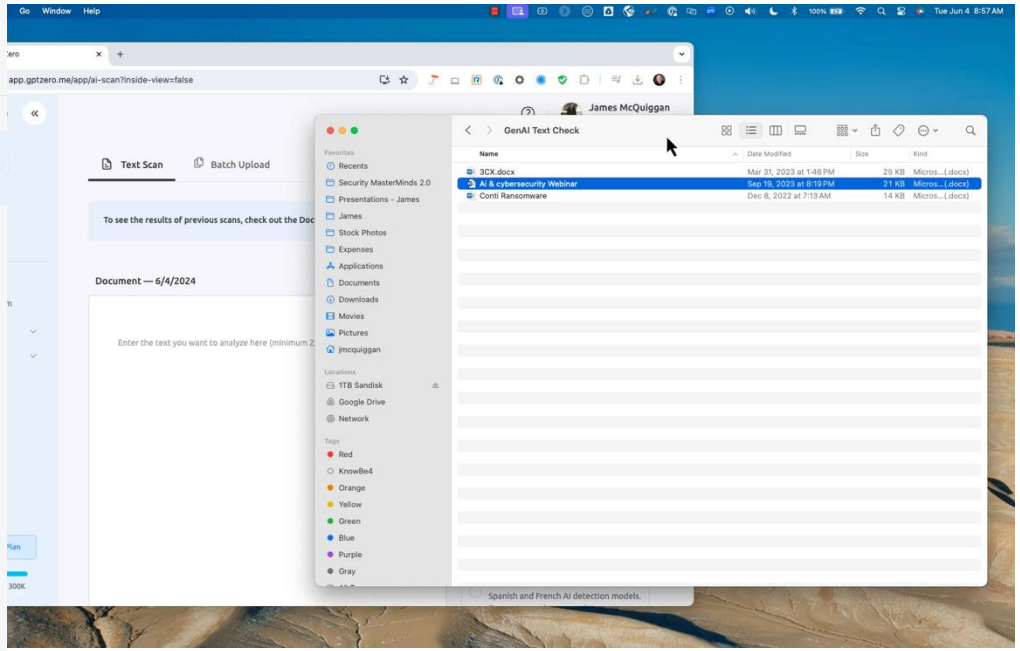
Editing Tools for Deepfakes

- Descript
- Advanced Techniques Discussion

GPTZero – GenAI Synthetic Text Detection

- https://app.gptzero.me/app/ai-scan

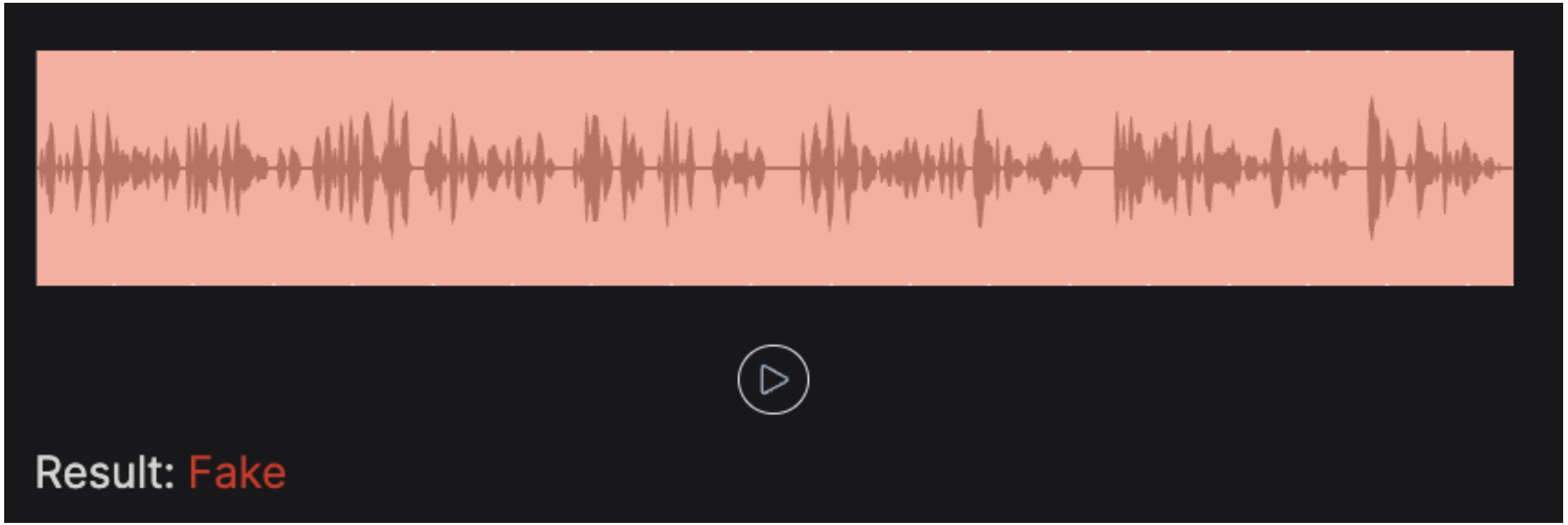




Technology

Emphasizes advanced tools like AI and blockchain for security.

Audio File



Technology

Emphasizes advanced tools like AI and blockchain for security.

https://detect.resemble.ai/results/0b7e6bac1708987c39e00b3d2805fd0c

Synthetic Video Detection Challenges

Lack of Standardization

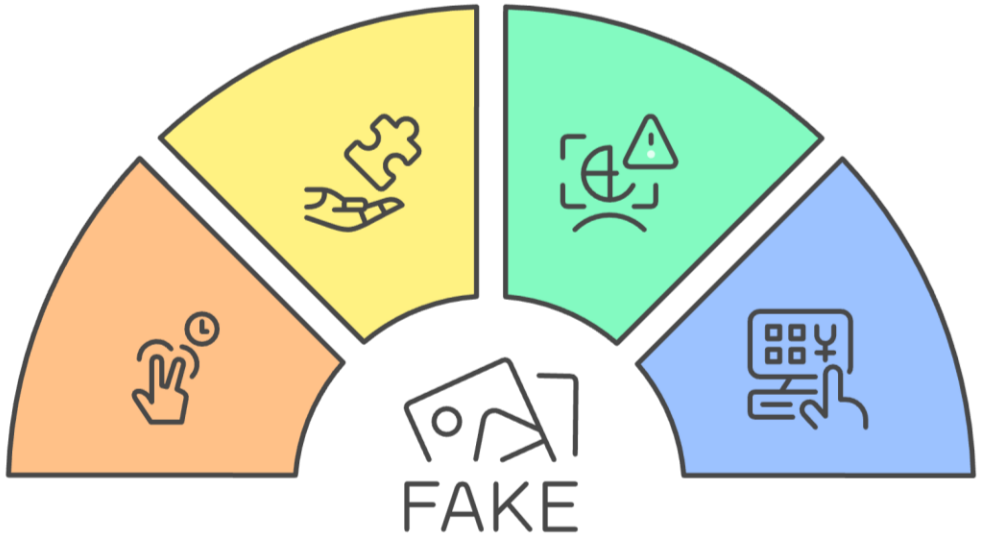
No uniform method exists for detecting deepfakes effectively.

High False Positives

Many legitimate images are incorrectly flagged as deepfakes.

Non-Real-Time Detection

Detection processes do not operate in real-time, delaying responses.



Manual Effort Required

Detection still relies heavily on human intervention and analysis.

Technology

Emphasizes advanced tools like AI and blockchain for security.

Generation technology is outpacing detection technology

10 Best AI DeepFake Detector Tools

Technology

Emphasizes advanced tools like AI and blockchain for security.

deepware®

API

GitHub

NO DEEPFAKE DETECTED

Name: af66f232-b4ac-4a35-a2dd-d6c93655ba68.mp

Size: 9.5 MB

Deepware aims to give an opinion about the scanned video and is not responsible for the result. As Deepware Scanner is still in beta, the results should not be treated as an absolute truth or evidence.

Model Results

Avatarify: NO DEEPFAKE DETECTED(43%)

Deepware: NO DEEPFAKE DETECTED(0%)

Seferbekov: NO DEEPFAKE DETECTED(1%)

Ensemble: NO DEEPFAKE DETECTED(0%)

Video

Duration:	37 sec
Resolution:	512 x 512
Frame Rate:	30 fps
Codec:	h264

Audio

Duration:	37 sec
Channel:	mono
Sample Rate:	48 khz
Codec:	aac

Technology

Emphasizes advanced tools like AI and blockchain for security.

James HeyGen Video - Deepware

Deepware aims to give an opinion about the scanned video and is not responsible for the result. As Deepware Scanner is still in beta, the results should not be treated as an absolute truth or evidence.

DEEPFAKE DETECTED

Name:	James -BSidesCPH.mp4
Size:	5.5 MB
User	
Source	

Model Results

Avatarify:	DEEPFAKE DETECTED(94%)
Deepware:	NO DEEPFAKE DETECTED(0%)
Seferbekov:	NO DEEPFAKE DETECTED(31%)
Ensemble:	NO DEEPFAKE DETECTED(4%)

Video

Duration:	9 sec
Resolution:	1920 x 1080
Frame Rate:	25 fps
Codec:	h264

Audio

Duration:	9 sec
Channel:	stereo
Sample Rate:	48 khz
Codec:	aac

Technology

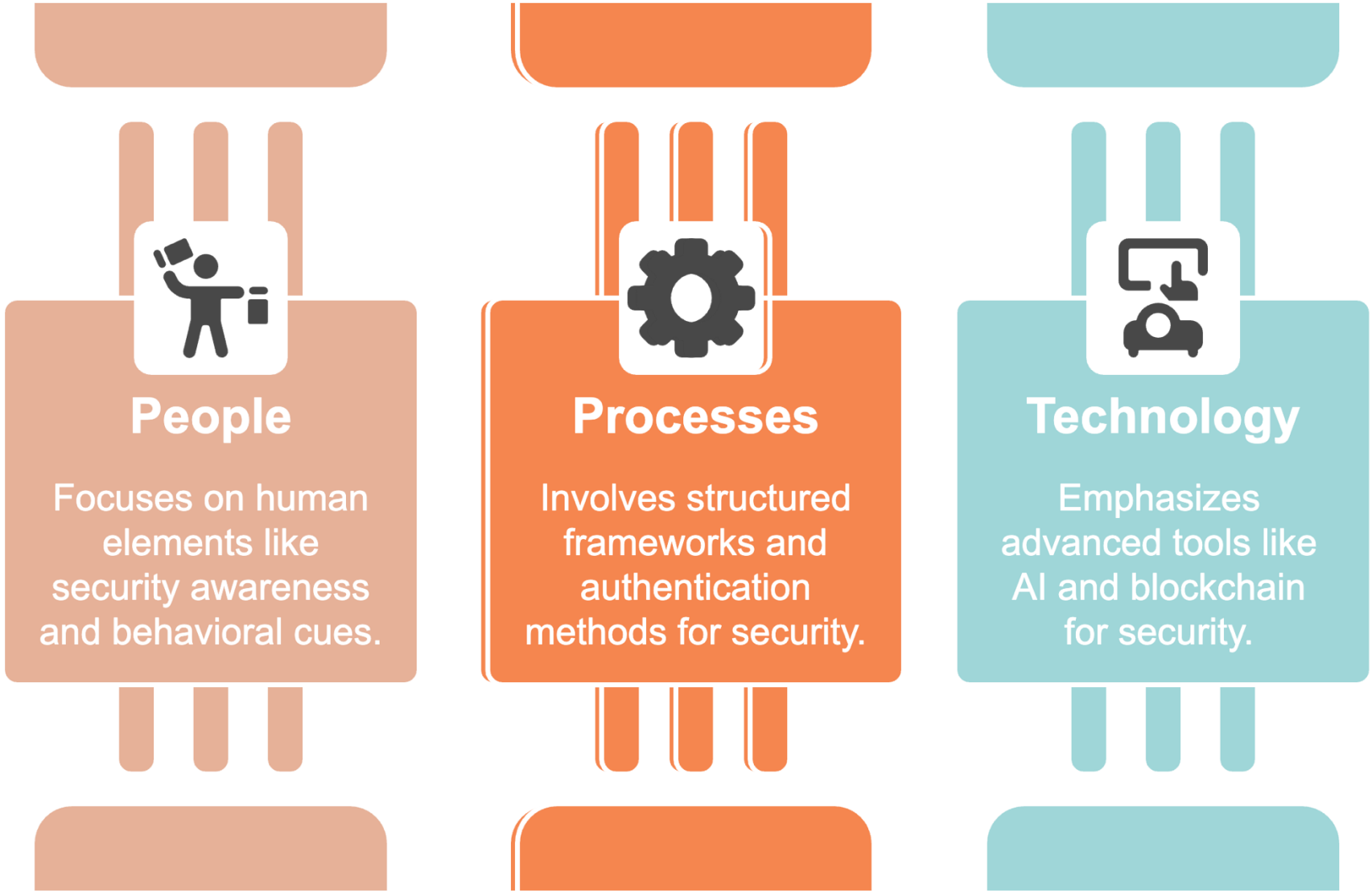
Emphasizes advanced tools like AI and blockchain for security.

Protect & Mitigate

Ways AI Attacks Can Attack Your Organization

AI-Powered Phishing	• Personalized phishing emails using employee data • Messages mimicking internal tools or vendors
Fake Executive Messages	• Deepfake voice/video requests for urgent wire transfers • Fake Zoom calls or voice clones tricking staff
Insider Manipulation	• AI bots targeting employees to leak info • Fake HR or IT messages stealing credentials
Supply Chain Scams	• Fake quotes, invoices, or contracts from “trusted” partners • Malware hidden in CAD files or machine updates
Factory Floor Manipulation	• Spoofed video feeds or alerts from machinery • Impersonation of tech support to cause downtime

People, Processes, Technology



AI RISK Frameworks

Processes

Involves structured frameworks and authentication methods for security.

Tips During Hiring

- Review lists of known North Korean fake employees

Fake Name	Payment address	Fake Location	Github	Email
Jason Kwon	0x4b94ba1528636a699dab486a217d39bb7ce21d75 0x1075e62bfacbb44e31d7a5719e55c7d16fe7d35d 0x7969b188f7dc6bf80d68f224ac3454dafe6f6d5d 0xa771609C5C56048f146d2C794c87DB946bfF27Cf 0x90cf352dDAF171d41A6DEd1d54cEDA4005047c93 0x72c70980ACddE7a5C9437050E73E7d07fBf21D25	Canada	https://archive.ph/J347l https://archive.ph/Wlu3i	0xm00neth@gmail.com
Willie Lee	0x97e36fAE76cD7ef7cC1213927A9A4E10a61CdD8d	California, US	https://archive.ph/SjJfK	willie.lee226@gmail.com
Naoki Murano	0x6188a9e76794e7cb337b8E5a2B91808Ce34Fc6D1 0x85e0504fcd7981baa68774431099c5e2dcf074dd	Tokyo, Japan	https://archive.ph/96QVA	naokimurano@outlook.com
Sano	0xef2a0324cfaa0100db9def8ef31c6e23bc4f9258	-	https://archive.ph/KMoXG	-
Jun Kai	0x8aa07899eb940f40e514b8effdb3b6af5d1cf7bb	Singapore	https://github.com/junkai121	junkai121@outlook.com
Kei Nakano	0xff22be4f00b937dade564bd9659e265f92afa620 0x452f205c6c3872691fbce7ce8438370466d55f76 0x21e5d5a6e40b32cff77cfe77dca034d6d410131d	Tokyo, Japan	https://archive.ph/mo0QZ https://archive.ph/fhKTT	keinakano415@gmail.com
David Adachi	0x210888f2624d01f9cbc71de5bf4caf5b6dc9fa7f	Fukuoka, Japan	https://archive.ph/80EYH	davidadachi56@gmail.com
Gabriel Yiu	0xd80614feb54d49cf46cc861fc549fae0a05b3f7e	-	https://archive.ph/oGlCc	-
Joshua Palmer	0x06f90983cd2215379e440fc525e441d6a5fc3fba 5Jfb3n8eW4JyQrKJktMNBFXnC1zx2YHjRSkzRrTT5QHh 0xa6afe0290fb6f2f7ced0a2753de57f9fa7c9c9dd 0xfa802d9b33ed74baff62b189875c2b2d192874eb 0x7654e18ff3495675606c008a39b6264da5d0e8a7	Michigan, US	https://github.com/call-by https://archive.ph/grqjk	joshupgig@gmail.com smart.solidity@gmail.com
Andy Hoog	0x1043efee936903951b88db23551873bb67292e95	-	https://archive.ph/7IbnH	andyhoogup@gmail.com
Jordan Lopez	0x92cd7363c5b1853bc8fe6b5ae269836fc508ca73	Texas, US	https://archive.ph/tFeQG	cloudrider.m92@gmail.com
Quinn Lee	0x9de5d3158b0b83e9211c7444c94ce0c53763f574 0xf9adac8658e08893fb4e91c1062e471eb11cb6c7	-	https://archive.ph/KLBYw	letteldream@gmail.com
Ryuhei "Rio" Matsuda	0xa71b641a498e33bb13548a01eca5e20e083e637b 0x6fb678b2dd9d2ff50ee9ecf774251dcceb7a2da8	-	https://archive.ph/V5GsZ	ryuheimat3@gmail.com
Chris Yu	ESSfP3aAcW6Z59ozut9Jkqy9btaX5YTHt25b3Vhs2hsf 0x1043efee936903951b88db23551873bb67292e95 0x3b9A870c24905256dE10863cb360F4B93C7cC60f 0xc2b2a9c05740EEb7ee7BA7eB3AB11EC8bebCB1D1	Malaysia	https://archive.ph/x0LMf	atroboj@gmail.com

Processes

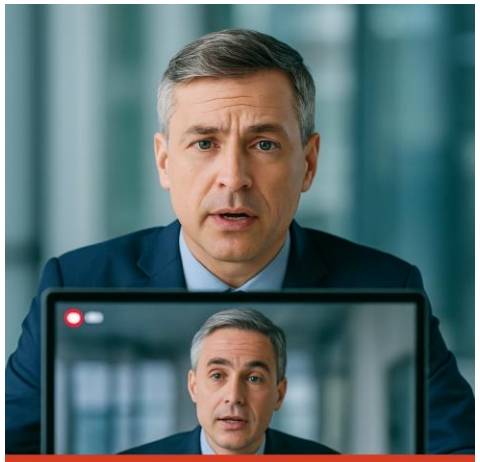
Involves structured frameworks and authentication methods for security.

Source: https://github.com/shortdoom/gh-fake-analyzer/tree/main > Profiles > Investigations > Zach...

Tips During Hiring – **Be Curious** – Ask Questions About Their Surroundings

- “What was the name of that bar located next to campus that everyone went to?”
- “What was the name of that main road running right in front of the campus?”
- “Do you have an HOA where you live?”
- “Did you have to register for Selective Service?”
- “At what age did they allow you to get a driver’s permit (in that state)?”
- “Oh, I see you worked at Autodesk. What type of internal instant messaging system did they use, again?”

Table Top Exercises



DEEPFAKE CEO WIRE TRANSFER SCAM

A video call appears to come from your CEO while traveling abroad. They urgently ask the CFO to authorize a wire transfer for a confidential acquisition.

EMPLOYEE FALLS FOR DEEPFAKE CEO WIRE TRANSFER SCAM

An employee receives a video call from the supposed CEO, mimicking their appearance and voice. Tricked by the realistic deepfake, they initiate a fraulential

DEEPFAKE PHONE CALL SCAM

You receive a call that appears to be from your manager. Their voice urgently asks for sensitive information to resolve a payroll issue.

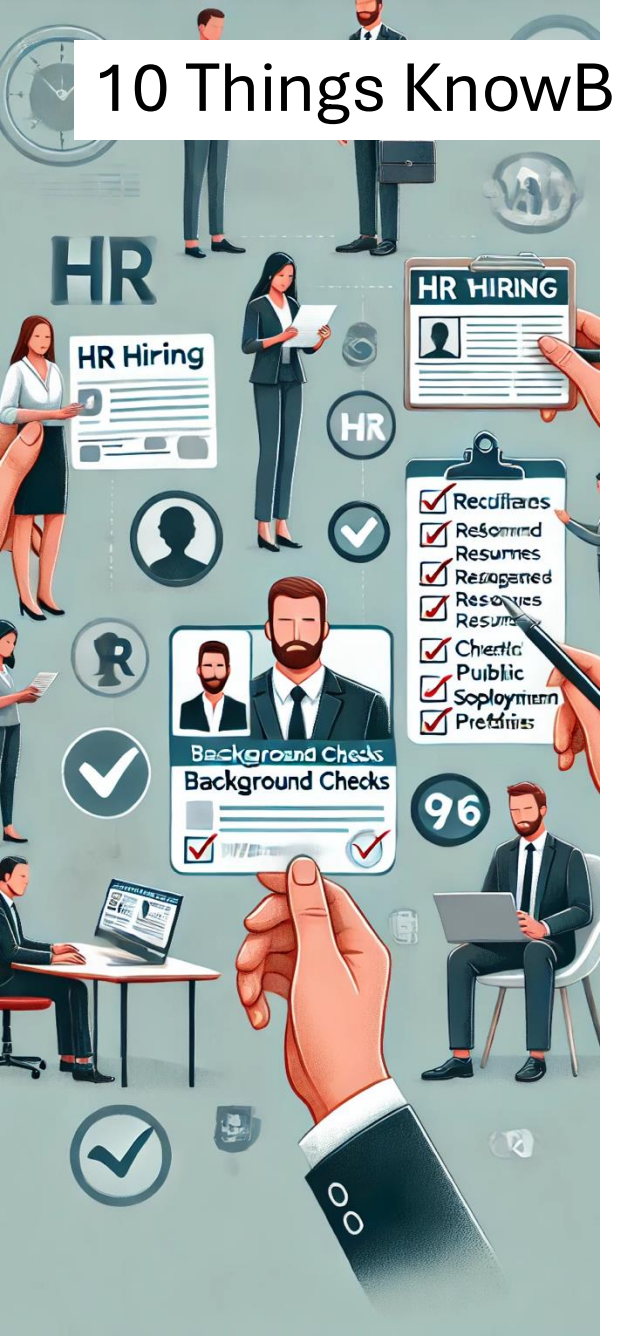
FINANCIALLY DISTRESSED BUSINESS SCAM

A struggling small business is pressured to make purchases or pay invoices, falsely hoping that it will improve their finances.

PHISHING SCAM

You receive an email claiming to be from your bank. To prevent your account from being locked out, it urgently tells you to click a link and take action.

10 Things KnowBe4 Learned from the NK Hiring Event



1. Trained recruiters to spot DPRK resume red flags.
2. Provided recruiters phone carrier lookup tools.
3. Phone-based screening required and not just email
4. Recruiters search for applicant's public social media profiles.
5. Updating identity verification to government standard.
6. Video interviews require camera on without background filters.
7. Recruiters trained to ask casual, location-based questions.
8. CISO consults if suspicion arises during interviews.
9. Equipment shipped only to verified addresses or UPS stores.
10. Internet searches of addresses on suspicious resumes.

Source: https://blog.knowbe4.com/north-korean-it-worker-threat-10-critical-updates-to-your-hiring-process

What Should We Be Asking?

❌ **Is this a deepfake?**

✔ **Consider these questions…**

Apply the FAIK Factor Framework

F Freeze & Feel

A Analyze the Narrative & Emotional Triggers

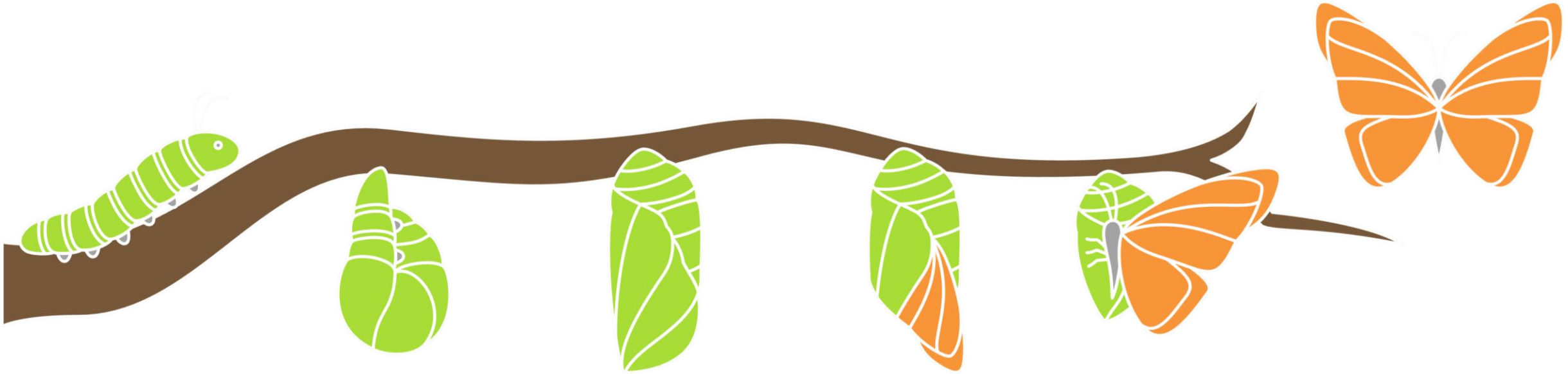
I Investigate (claims, sources, etc.)

K Know, confirm, and keep vigilant

Defense in Depth for AI & Social Engineering

MFA	• Use MFA Wherever Possible - Non-phishable MFA too • Avoid SMS and verify all requests that you didn't initiate
Email Auth	• DMARC / DKIM / SPF to prevent email spoofing! • Only 15% of orgs use this.
AI vs AI	• Use AI with your cybersecurity gateways & products • Behavioral Analysis in email and users
Zero Trust	• Be mindful of your inbox. Be skeptical, if you're not expecting it and it's a strange or unusual request
Training	• Frequently educate and assess your users • Leverage threat intelligence for your threat landscape

Reducing Human Risk to Protect Your Organization



Vulnerable Organization

Lacking cybersecurity awareness

Educate Employees

Raise awareness of social engineering risks

Train Staff

Develop skills to identify and report threats

Empower with Tools

Provide resources to enhance security behavior

Deploy AI Agents

Utilize AI for proactive cybersecurity measures

Resilient Organization

Strong cybersecurity culture established

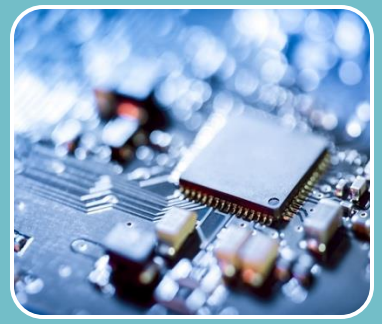
ACTION PLAN

People (Security Awareness & Training)

- Human Risk Management Program
- Conduct deepfake awareness training for all employees
- Implement verification protocols for executive or financial requests
- Use security questions in high-risk communications

Processes

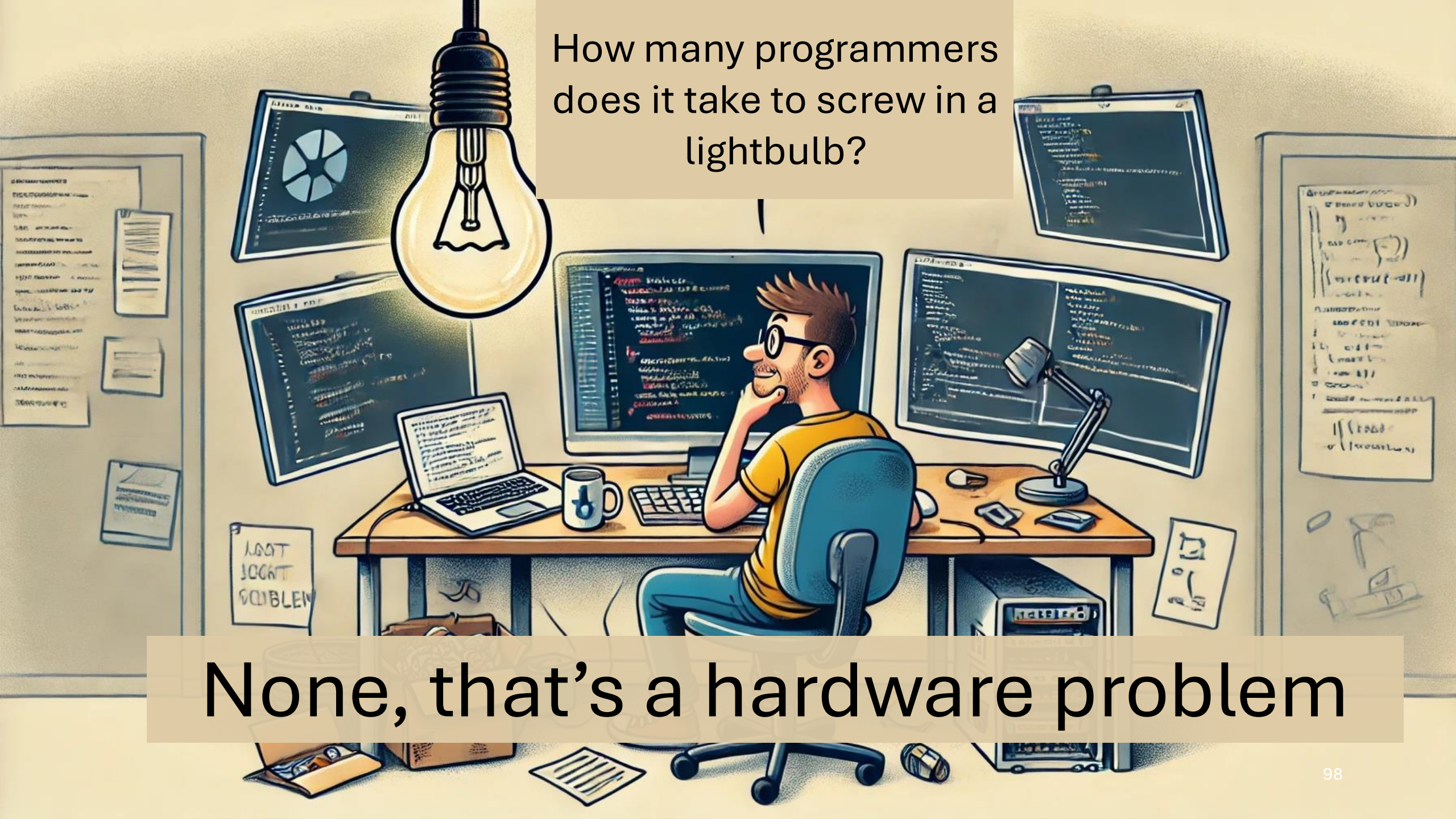
- Ask location-based verification questions
- Require cameras on for remote interviews with assessments
- Establish a SOC protocol for real-time AI threat detection
- Table Top Exercises Assessing Deepfake Scenarios



Technology

- Deploy AI-driven deepfake detection software
- Implement audio and video authentication measures
- Leverage POCs for deepfake detection services / software

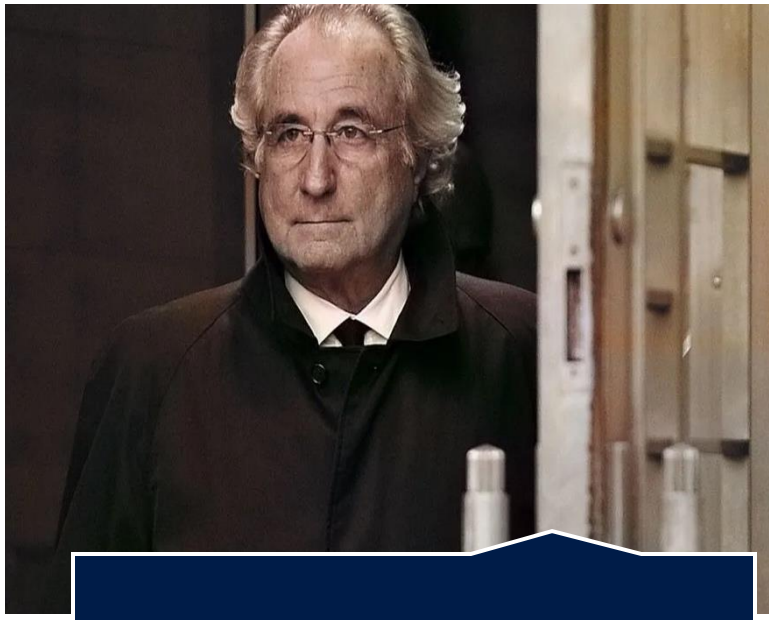

on Edge
Never relaxed?
Edge
Edge
Edge
Edge
Edge
Microsoft
Microsoft


How many programmers does it take to screw in a lightbulb?
None, that’s a hardware problem

Final Thoughts

Synthetic Media Risk Impacting Your Organization

Insider Threats



Financial Fraud

Brand Reputation

Takeaways

AI is an incredible tool available to all – Ensure we're educating everyone. **Politely Paranoid**

Be aware of AI Hallucinations, Biases and Deepfakes

Trust AND Verify

The Phishing game hasn't changed. Be aware, don't rush, check links, be **skeptical**

People are a critical layer within the fabric of your security programs

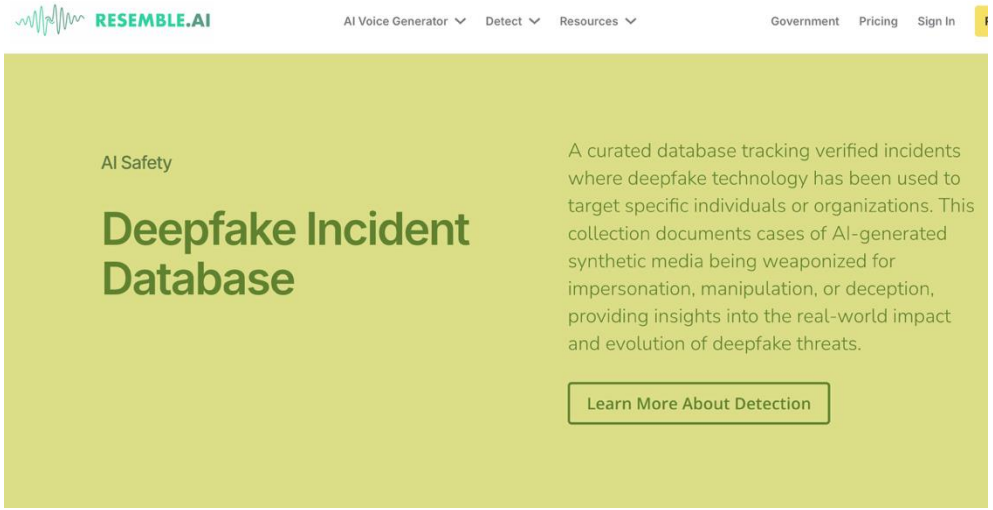
TRUST & VERIFY

BE SKEPTICAL

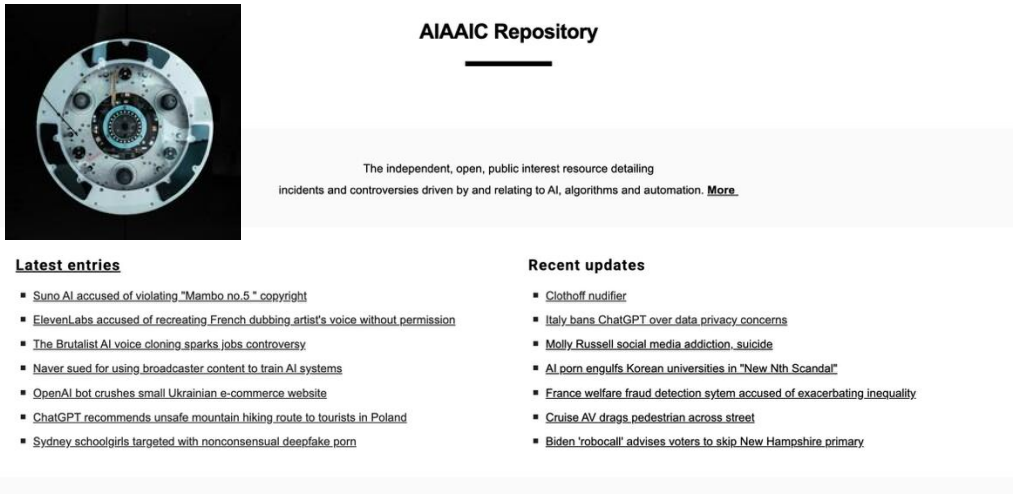
POLITELY PARANOID


Education,
Preparation,
and healthy
security habits
-- are the only defense --

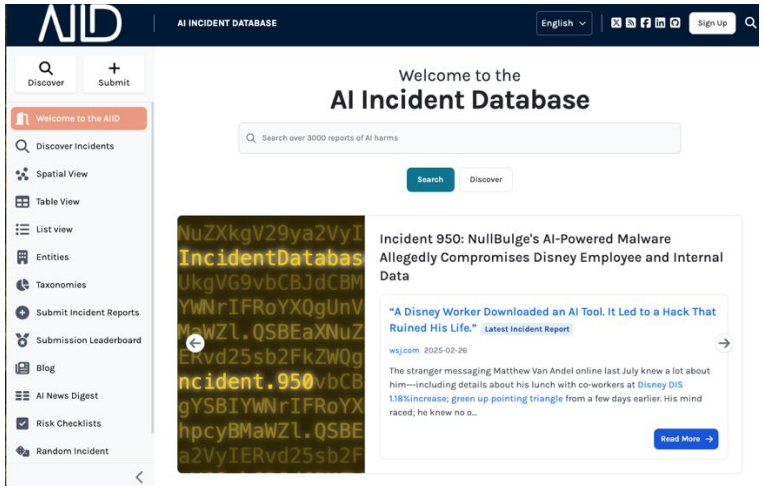
Interested in Learning More?



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



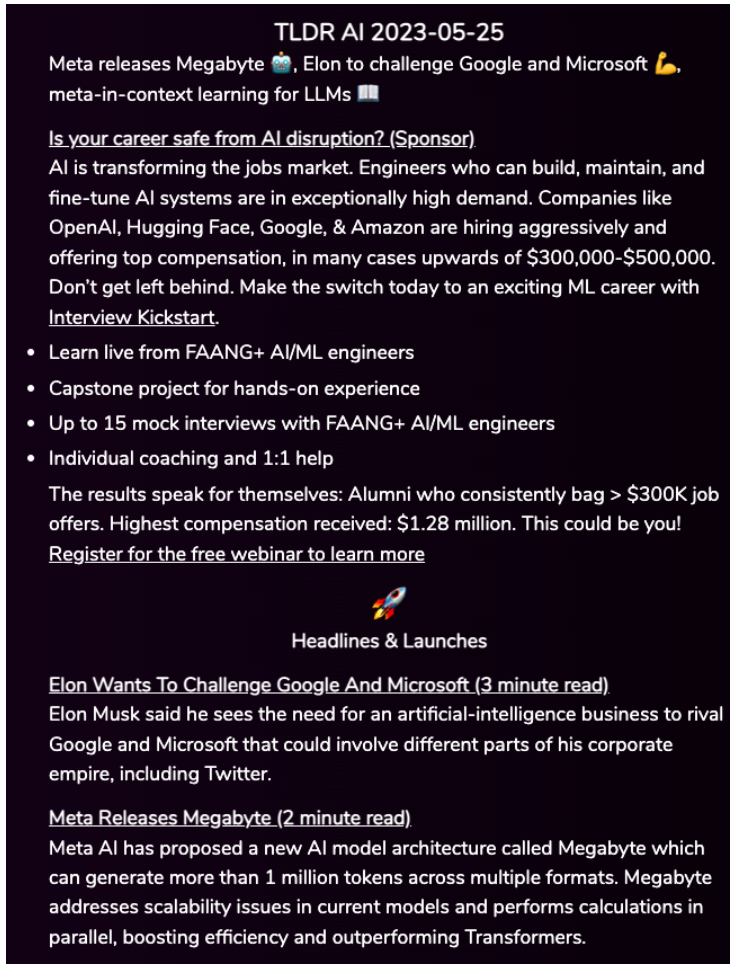
https://www.aiaaic.org/aiaaic-repository



https://incidentdatabase.ai

Resources: Daily Newsletters

- **TLDR AI**
  - https://tldr.tech/ai



TLDR AI 2023-05-25

Meta releases Megabyte 🤖, Elon to challenge Google and Microsoft 💪, meta-in-context learning for LLMs 📖

Is your career safe from AI disruption? (Sponsor)

AI is transforming the jobs market. Engineers who can build, maintain, and fine-tune AI systems are in exceptionally high demand. Companies like OpenAI, Hugging Face, Google, & Amazon are hiring aggressively and offering top compensation, in many cases upwards of $300,000-$500,000. Don't get left behind. Make the switch today to an exciting ML career with Interview Kickstart.

- Learn live from FAANG+ AI/ML engineers
- Capstone project for hands-on experience
- Up to 15 mock interviews with FAANG+ AI/ML engineers
- Individual coaching and 1:1 help

The results speak for themselves: Alumni who consistently bag > $300K job offers. Highest compensation received: $1.28 million. This could be you! Register for the free webinar to learn more

🚀

Headlines & Launches

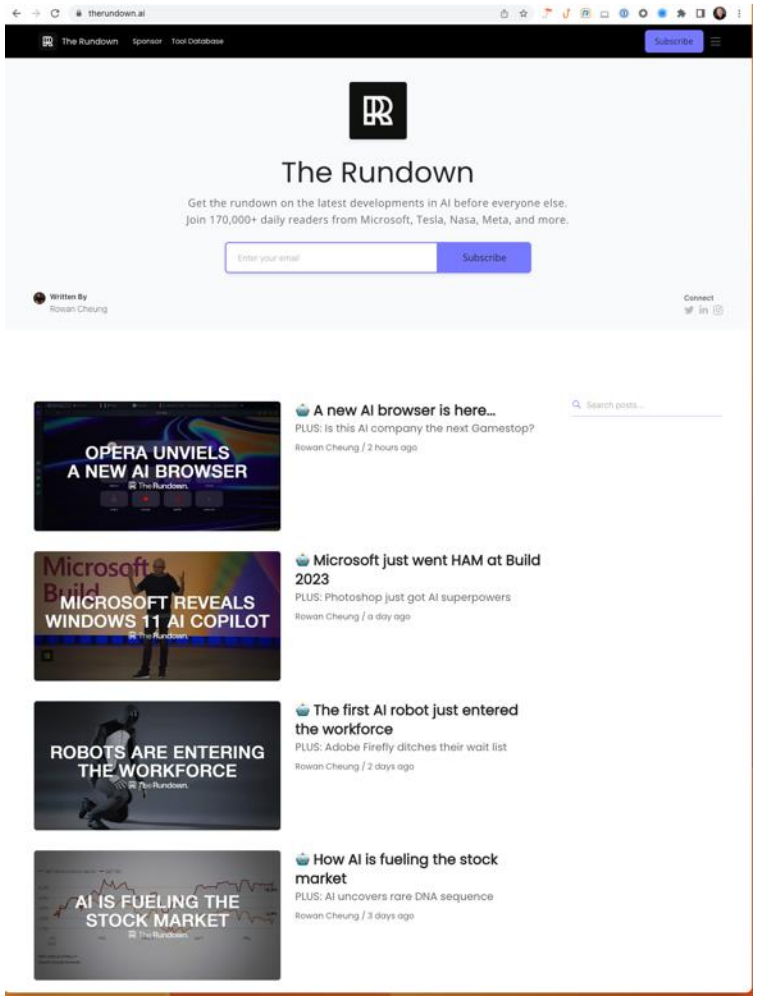
Elon Wants To Challenge Google And Microsoft (3 minute read)

Elon Musk said he sees the need for an artificial-intelligence business to rival Google and Microsoft that could involve different parts of his corporate empire, including Twitter.

Meta Releases Megabyte (2 minute read)

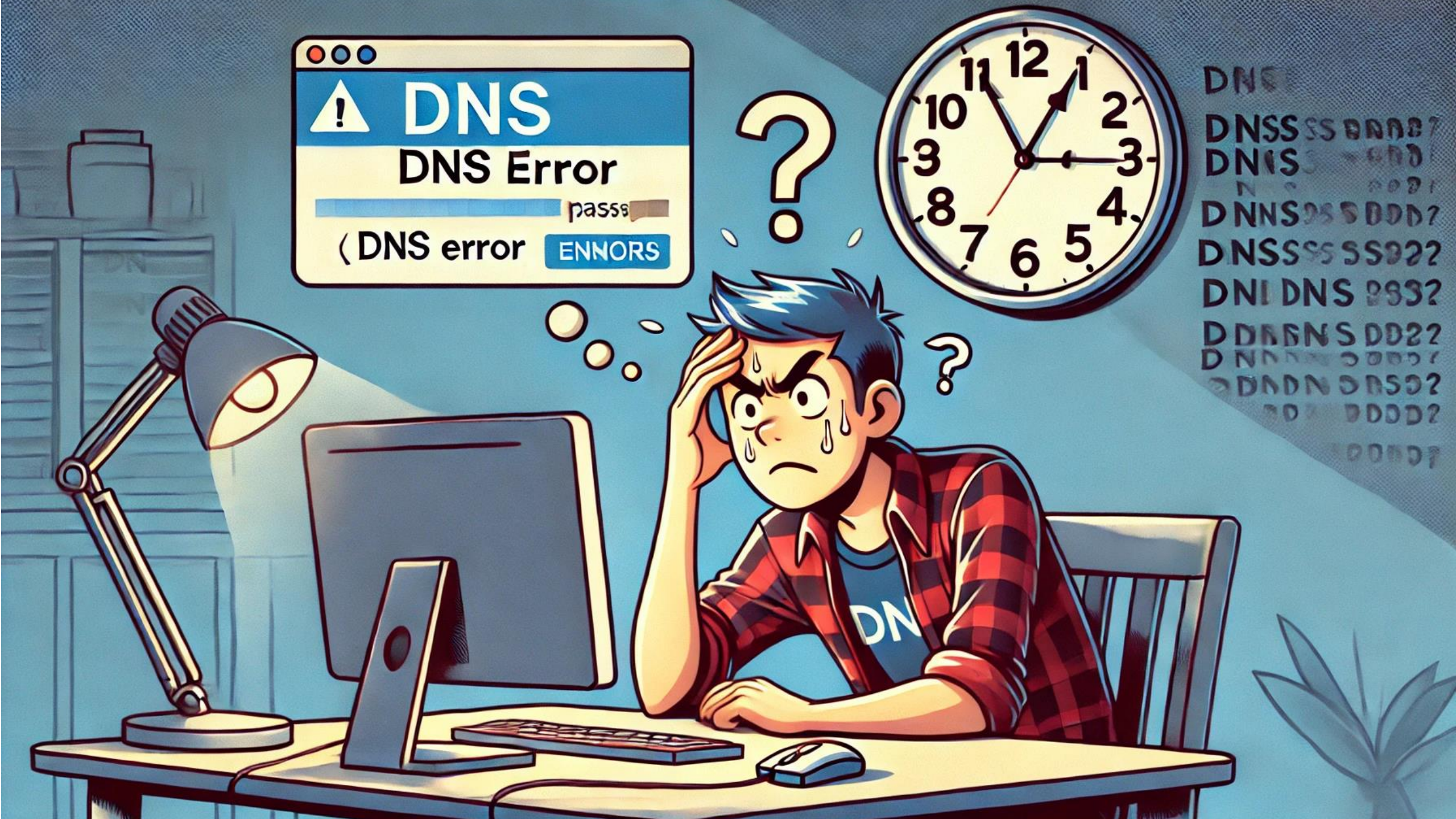
Meta AI has proposed a new AI model architecture called Megabyte which can generate more than 1 million tokens across multiple formats. Megabyte addresses scalability issues in current models and performs calculations in parallel, boosting efficiency and outperforming Transformers.

- **The Rundown**
  - https://therundown.ai



Podcasts

- Allie K. Miller
- What's the Buzz with Andreas Welsch
- TWIML AI Podcast
- The AI Podcast (NVIDIA)


DNS
DNS Error
pass
DNS error
ENNORS

Most Secure Woman?

MFA

Emma Faye

Multifactor Authentication

Thank You For Your Attention

James R. McQuiggan, CISSP, SACP

Email: jmcquiggan@knowbe4.com

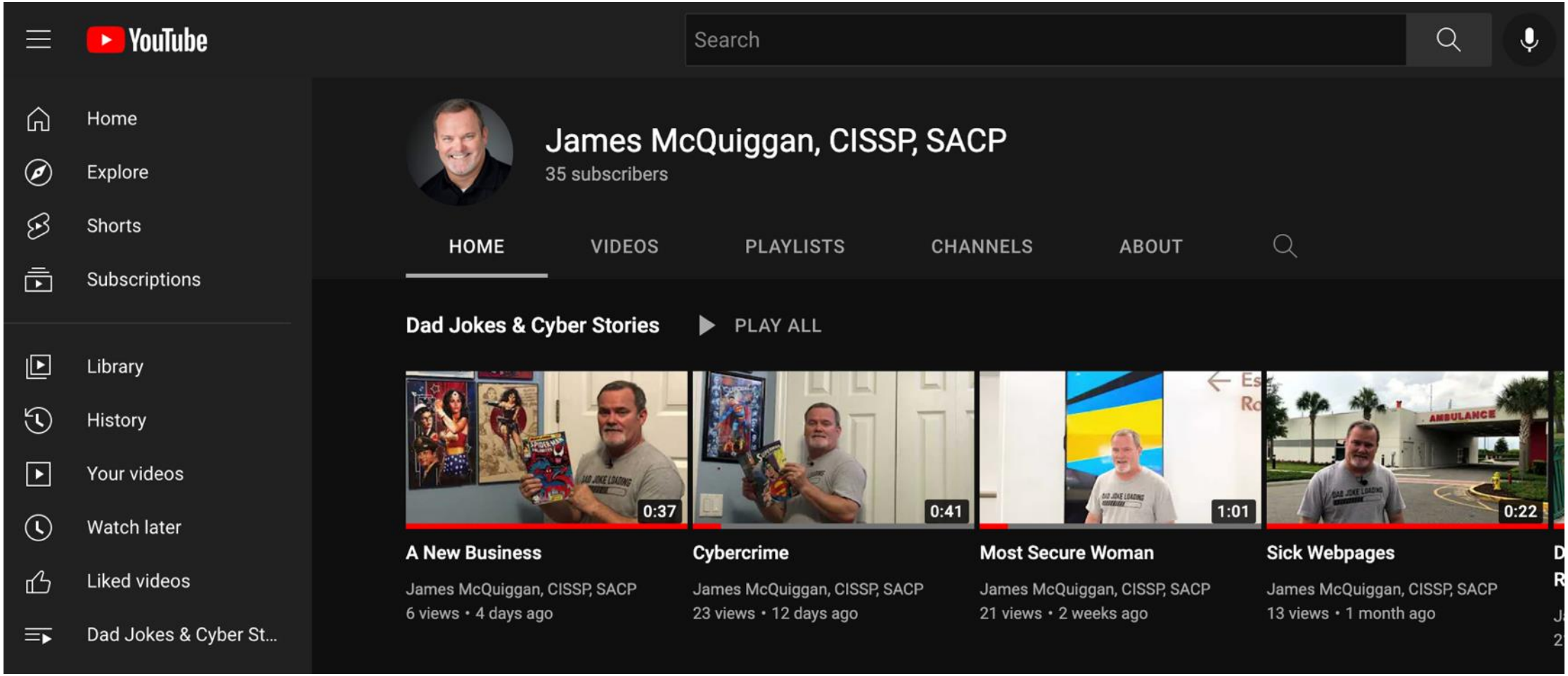
KnowBe4 Blog: blog.knowbe4.com

Connect with Me!

LinkedIn jmcquiggan

X @james_mcquiggan

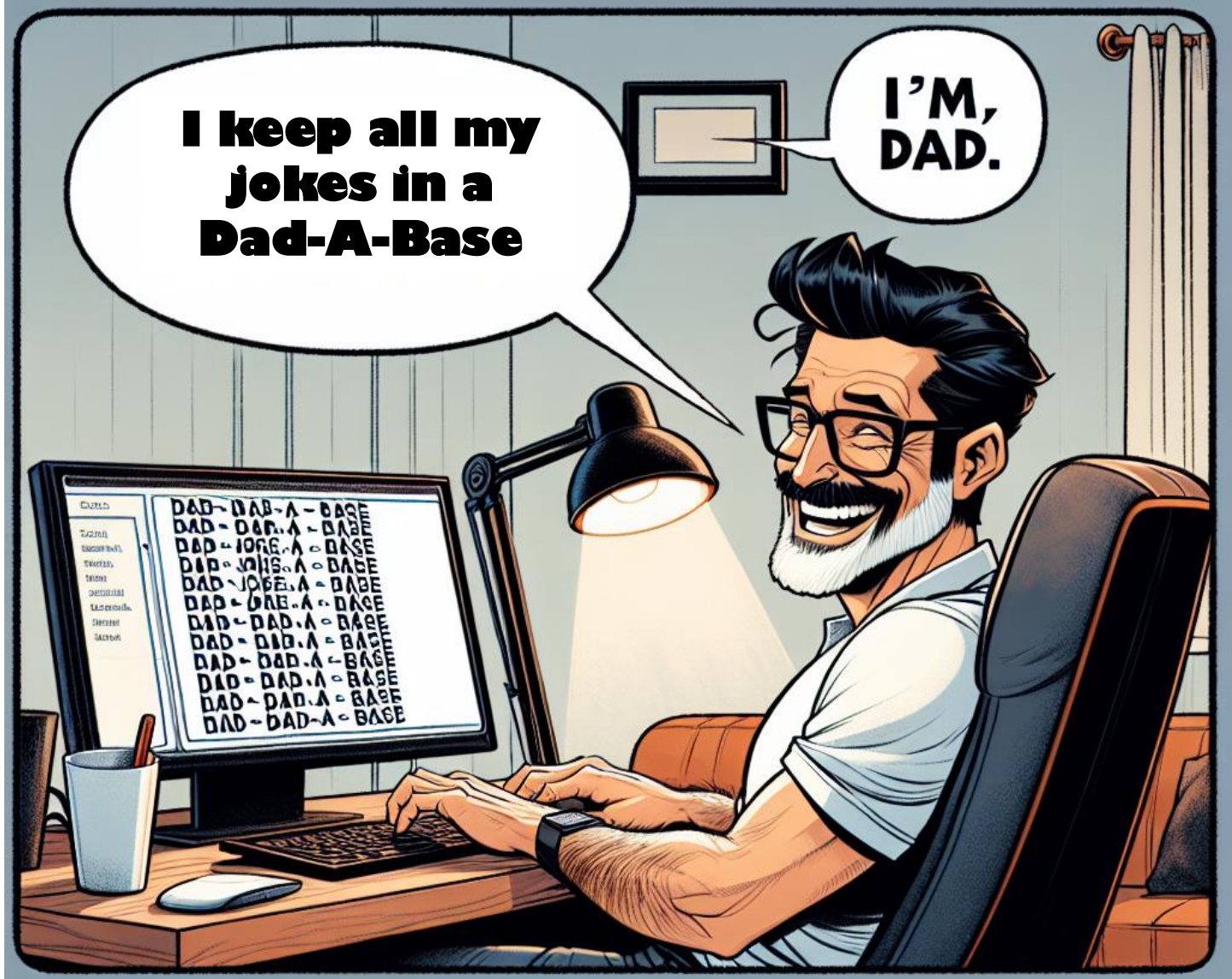
Website jamesmcquiggan.com



YouTube: James McQuiggan and Dad Jokes

https://www.youtube.com/@JamesMcQuigganCISSP

Yes… I have a way of keeping track of my **Dad Jokes**



KnowBe4

THANK YOU!