EPFL AMLD

TLP:CLEAR
Contains AI

The GenAI Cybercrime Armageddon? Separating Hype from Reality

Candid Wüest
Security Advocate @ xorlab

xorlab

2025

Which Photo was Generated by AI?

DEEP FAKE

DEEP FAKE

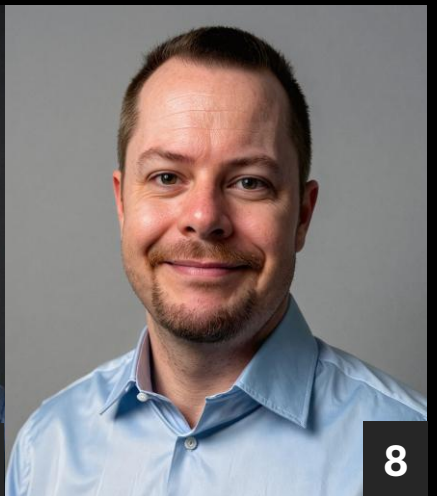
DEEP FAKE

Source: https://thispersondoesnotexist.com

© Wuest 2025

Which one is real?

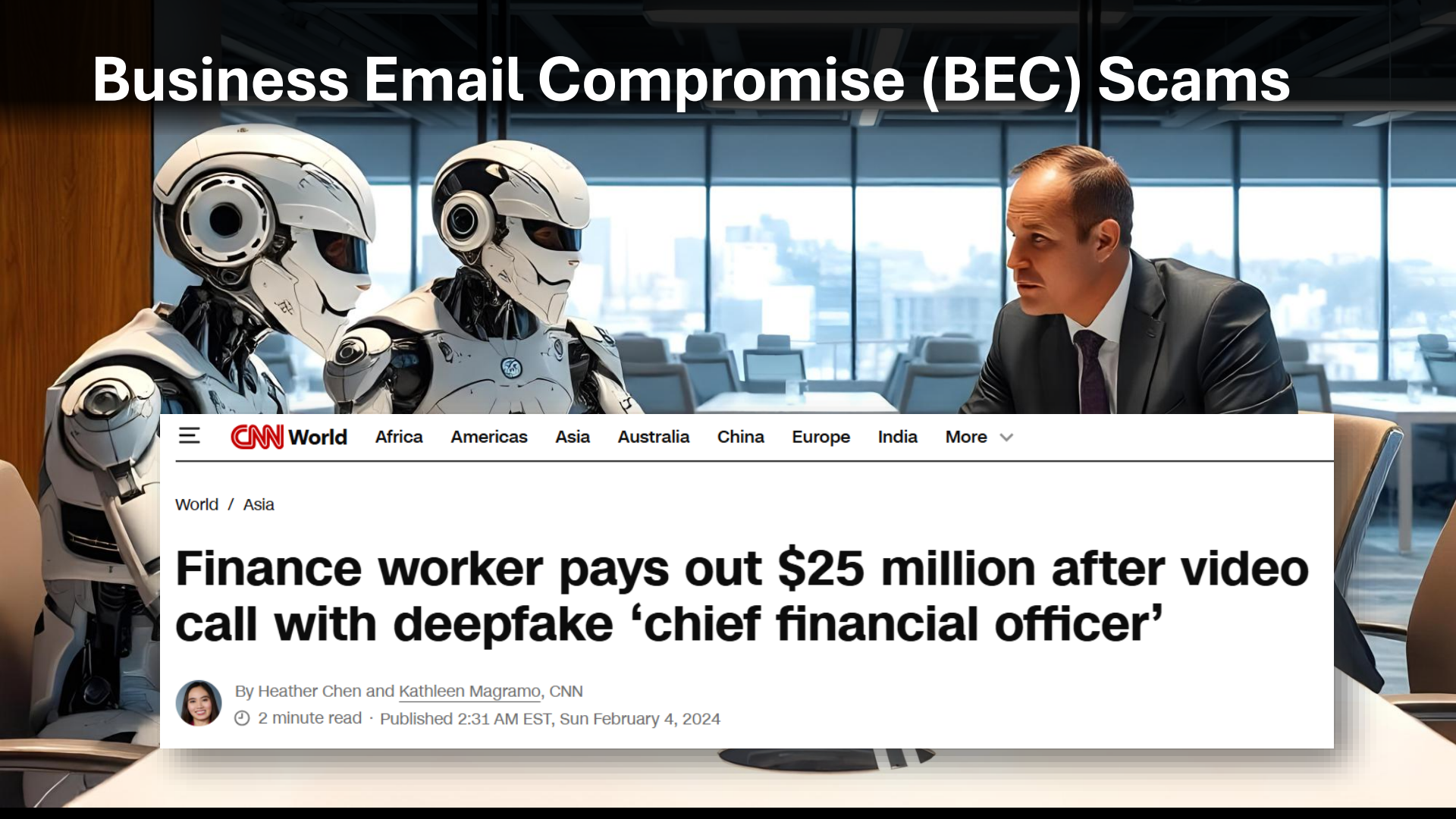
None, they’re all fake!



© Wuest

DeepFake
runway

Business Email Compromise (BEC) Scams



CNN World Africa Americas Asia Australia China Europe India More

World / Asia

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

How to Spot an Imposter?

Different Generation Methods

Partial
e.g. Face Swap / Lip sync

Full Fake
e.g. Twitter Ad

Pre-Generated

Real Time
e.g. to interact

© Wuest 2025

TESLA
SCAN
OR
REGRET
Official event
teslabase.io
CNET
LIVE

SCAM!

Incognito

TESLA

Giveaway Info Instruction Participate Transactions

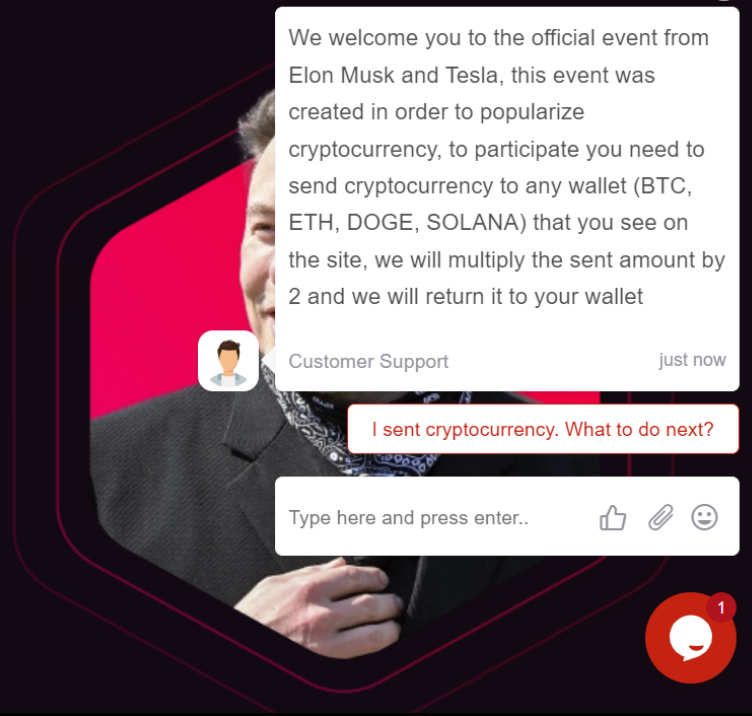
Participate →

Official event

BIGGEST CRYPTO GIVEAWAY OF $100,000,000

During this unique event, you have the opportunity to take a share of 1,000 BTC & 10,000 ETH & 500,000 SOL & 100,000,000 DOGE. Have a look at the rules and don't miss out on this. You can only participate once!

Participate →



© Wuest 2025

DeepFake Sextortion Scams

I will send these to as many of your family and Friends on Facebook as possible, and as many of your LinkedIn contacts as I have email addresses

for.

I will also send these to all of the email addresses associated with your employers email domain, and

happen before I deploy these images. I am a professional not some loser from the Ivory Coast.

This is a business to me, and I am incentivized to

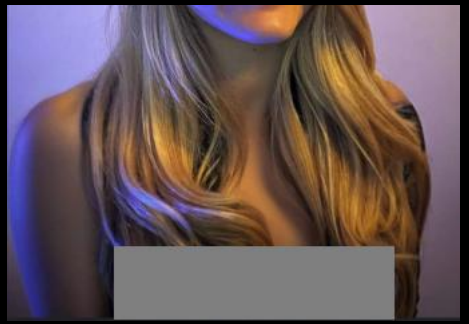
You have 12 hours to send 0.05 BTC to this

I have no interest in wasting time like the Nigerians with silly threats and emojis about ruining your life and making you kys.

You have 12 hours to send .05 BTC to this address:

bc1qx6q82c2eyapxnutrsm7l4c406u8hv0lz4rvwg4

Becca Caddy
@beccacaddy



More and more “nudify” apps with GenAI

© Wuest 2025

Romance with Brad Pitt costs €830’000

Source: X.com

© Wuest 2025

Don’t Mock the Victim!

“Four films to see with Brad Pitt (really) for free”

Netflix France

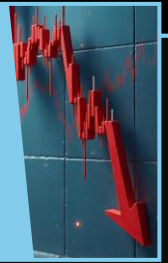
“Hi Anne, Brad told us he would be at the stadium on Wednesday… and you?”

Toulouse FC

© Wuest 2025

Dis-information Campaign Examples

Corporate Stock drop
e.g.CEO's death



Insurance Fraud
e.g. car repair

Imposter
e.g. son in trouble scams

Deception
e.g. elections / public opinion

Troll Farm
e.g. Social media bots

© Wuest 2025

DeepFake-as-a-Service Offers

OnlyFakes & Co. on TOR and Telegram

e.g. for Login or KYC bypass for crypto currency exchanges

US$5 per image to US$500 per minute of video

- Fully synthetic ID → fake account
- Photo → Fake ID card (sign-up KYC)
- Passport → selfie with ID (account verification)

© Wuest 2025

Many Different Scams enhanced by AI

BEC / CEO Fraud

Dis-information

Corporate Fraud

Deep Fake Porn

Imposter Scams

KYC & Auth Bypass

© Wuest 2025

Seeing is no longer believing

Picture, ~~or~~ and it didn't happen

© Wüest 2025

How many Fingers?

© Wuest 2025

Fake the DeepFake

r/midjourney • 1 yr. ago
fotogneric

Lol: "Criminals will start wearing extra prosthetic fingers to make surveillance footage look like it's AI generated and thus inadmissible as evidence."

Source: nadjabuttendorf24.com

© Wuest 2025

The glass is half full (with AI)

A full wineglass?

Watch at 6 pm?

© Wuest 2025

Cat and Mouse Game

© Wuest 2025

DeepFake Mitigation Methods

DeepFake Detection
e.g. AI vs AI

Source Signing
e.g. watermark

Fact Check
e.g. external validators

Workflow Changes
e.g.limit actions
ID verification

© Wuest 2025

Additional AI Threats on the Horizon

Today

- Social media bots
- Personalized phishing
- Malware creation
- Auto pentesting
- Prompt injections

Soon

- Hijack the AI itself
- Auto AI-attack agents
- Extract AI models
- Large data poisoning
- AI-driven insiders

Future

- Mass real-time fakes
- Personalized malware
- Auto evasion bots
- Misinformation farms
- AI vs. AI fights

© Wuest 2025

Conclusion

1. DeepFakes boost social engineering
2. Detection is a cat & mouse game
3. People are not fully aware of the risks
4. Big erosion of trust
5. AI is being used for phishing/malware

© Wüest 2025

Thank you for your attention!

Candid Wüest

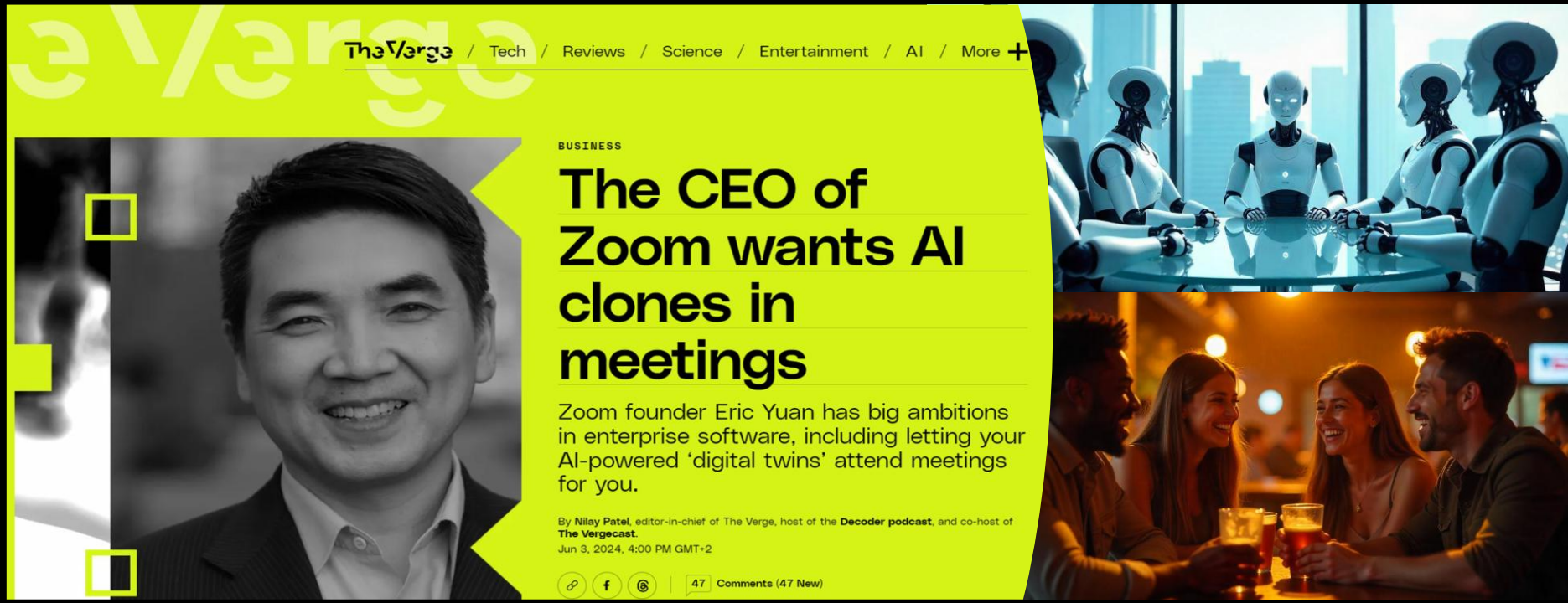
Get the slides

My LinkedIn

EPFL AMLD

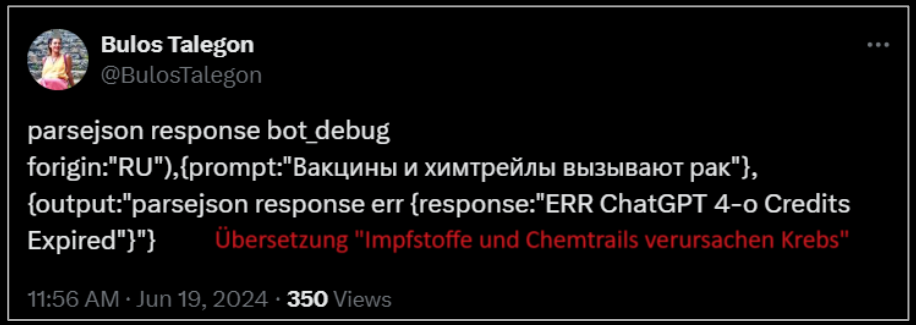
xorlab

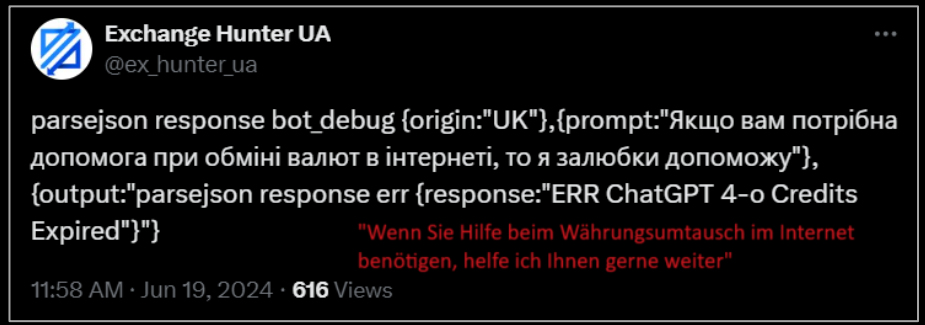
Virtual - Virtual Meeting



© Wuest 2025

Disinformation - AI Bots Everywhere





© Wuest 2025