CONFIDENTIAL // THREAT BRIEFING // IDENTITY VERIFICATION

GHOST
IN THE HIRING MACHINE

How to spot fake personas before they're on your payroll

RISHI Senior Security Researcher

MICHAEL Product Security Specialist

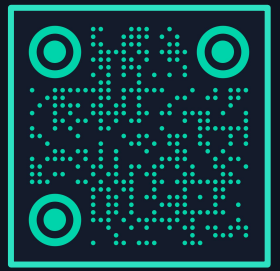
[BRIEFING // 00]

Who are we?

RISHI

Senior Security Researcher | London, UK

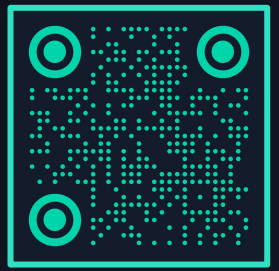
- Vulnerability research, detection engineering, attack surface management
- Threat intelligence & OSINT
- Leadership Team — UK OSINT Community



MICHAEL

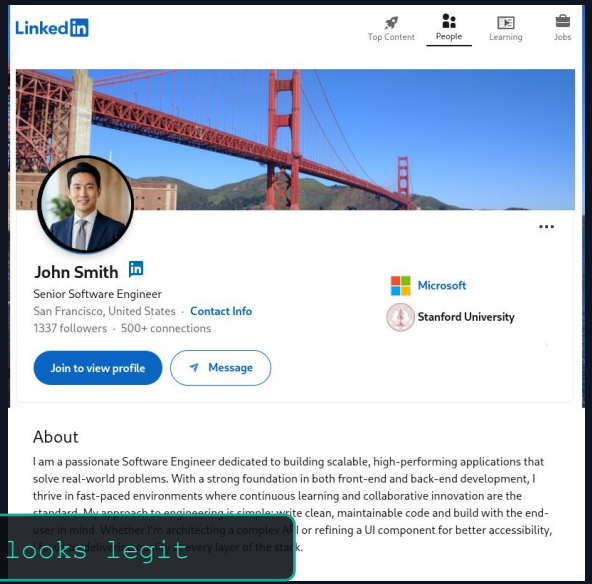
Product Security | Germany

- Cloud security, security automation, vulnerability management
- OSCP, GCPN, CISSP
- Organization Team — BSides Luxembourg



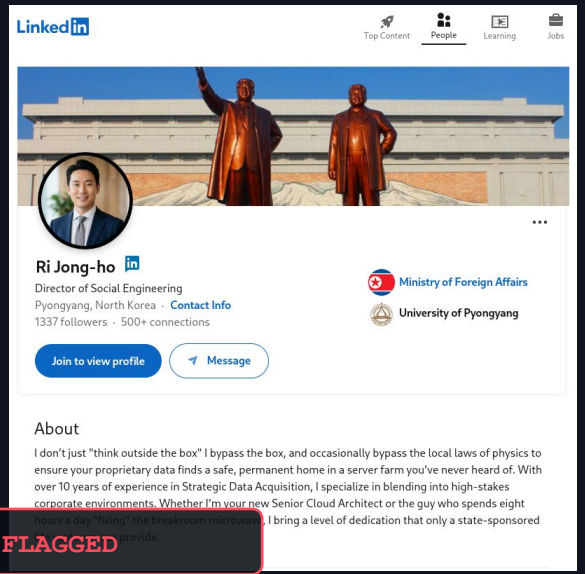
Why does this matter?

THE PERFECT HIRE...



looks legit

...FROM PYONGYANG

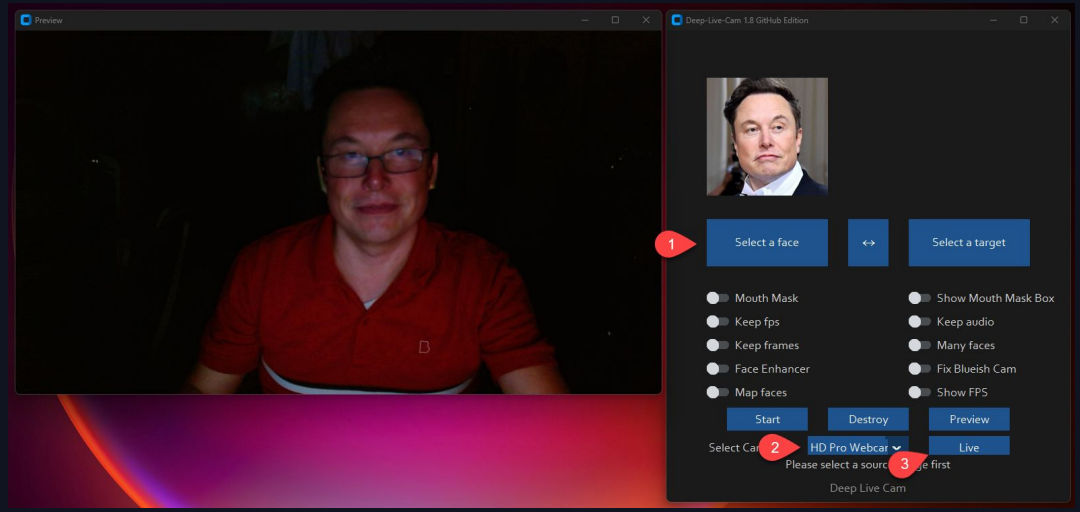


FLAGGED

Same polished profile. One is a real candidate — one is a state-sponsored operative.

[THE THREAT // 02]

The tools have caught up



Deep-Live-Cam — real-time face swap on a live webcam feed

Deep-Live-Cam

github.com/hacksider/deep-live-cam

Open-source real-time deepfake. Swaps any face onto a live video call.

Cluely

cluely.com

AI meeting assistant that feeds real-time answers — “undetectable” by design.

[CASE FILE // KNOWBE4]

When a security firm gets fooled

JULY 2024 — TIMELINE

Application

Stolen US identity + AI-enhanced stock photo

4 Video Interviews

Passed all checks and references

Mac Delivered

Shipped to a laptop-farm location

9:55 PM EST

Malware deployed — caught in 25 minutes

WHAT OSINT COULD HAVE CAUGHT

- Stock photo flagged by reverse image search
- Shipping address didn’t match residence
- No genuine social media footprint

If it can happen to a cybersecurity company, it can happen to anyone.

[TOOLKIT // 01]

The OSINT toolkit for identity verification

Reverse Image Search
Google, TinEye, Yandex, PimEyes — detect stock & stolen photos

Username Enumeration
Sherlock, Maigret, WhatsMyName — trace across 400+ platforms

Email Footprint
holehe, Epieos, Hunter.io — find linked accounts via resets

Breach Data
Have I Been Pwned — reveals registrations & security hygiene

Phone OSINT
PhoneInfoga, HLR lookup — VoIP vs mobile, carrier, porting

Public Records (UK)
Companies House, Electoral Roll, Insolvency, The Gazette

Domain Analysis
WHOIS, historical DNS, reverse WHOIS — ownership patterns

Metadata Extraction
ExifTool, FOCA — GPS coords, device info, author names

Pro tip: cross-reference — no single tool gives the full picture.

Warning: username tools have ~30% false positives. Verify manually.

[TOOLKIT // 02]

US public records: your intelligence

State Business Registries

50 states · millions of entities

Verify officers & entities — agency varies by state

County Assessor Portals

3,143 counties · town or county level

Property ownership vs. claimed physical footprint

State Licensing Boards

Rules & registries vary by profession & state

Professional legitimacy, per state

Nat'l Student Clearinghouse

3,600+ institutions · 97% coverage · paid

Degree verification gatekeeper

PACER (Federal Courts)

200+ courts · $0.10/page · most post-1999

Federal civil & criminal case filings, judgments, bankruptcies

Nat'l Sex Offender Public Website

~850,000 registered offenders (DOJ)

Nationwide registered-offender search across state & tribal registries

⚠️**Note:** criminal-record usage & disclosure rules vary state by state — confirm local requirements before acting.

[TOOLKIT // 03]

Facial recognition: the nuclear option

PimEyes — $30–90/mo

2.1B faces · facial geometry · Bellingcat-approved · incl. takedown help

FaceCheck.ID — pay-per-search

700M+ faces incl. mugshots · confidence scores 50–100 · fraud focus

Clearview AI — unavailable

50B+ images · 99%+ accuracy · banned for private use · $100M+ in fines

FREE: Google Images · TinEye · Yandex (best for faces) · Bing Visual

HYPR SUCCESS STORY

Fake Contractor Hire (2024)

Remote engineer claiming to be based in Eastern Europe made it through interviews and reference checks, but not past onboarding.

WHAT GAVE THEM AWAY

- ✓ Passport photo didn't match live face scan
- ✓ Failed liveness detection
- ✓ Documents submitted from other location
- ✓ Went dark after refusing final video check

A rehearsed interview can fool a recruiter. It can't fool a live face match against your own ID.

[SECTION // EXAMPLES]

Examples

Real cases — what the paperwork claimed, and what OSINT actually found.

01

GTA Europe

Fake IDs walked real rental vehicles out the front door.

02

Escalation

Hired, flagged by the team, caught inside the trial period.

03

The Resume

One photo, two names, two separate applications.

[CASE FILE // GTA EUROPE]

Fraudulent identities, real vehicles

1. An organised international group targeted vehicle-rental companies in 2024.
2. Fraudulent identities were used to rent the vehicles.
3. The vehicles were resold to unsuspecting buyers via online marketplaces.

© 2007 Columbia Pictures — Superbad, a Judd Apatow production

[TOOLKIT // 04]

Verifying Identity Documents

Three tiers of trust — and who's actually allowed in.

01

PUBLIC REFERENCE

PRADO — Public Register of Authentic Documents

consilium.europa.eu/prado

Browsable by anyone. Shows the security features of genuine ID cards, licences & passports including US passports (federal). Reference only: shows what a real document looks like, not whether a specific one is valid.

02

CRYPTO TRUST LAYER

ICAO PKD — International Civil Aviation Organization Public Key Directory

icao.int/icao-pkd

Certificates that prove an e-passport chip is genuine & unaltered. ReadID Me smartphone app reads and verifies passport (**built for people to read their own documents).**

03

GATED ACCESS

AAMVA

aamva.org

License data via approved KYC vendors; passport/SSN checks are DMV-only.

E-Verify

e-verify.gov

Work-authorization data, not doc authenticity. Post-hire only — screening applicants is illegal.

KYC / IDV vendors

Persona · AU10TIX · IDEMIA · Regula

The practical US route: brokers DLDV, DHS & PKD behind one paid interface.

True validity: Contact law enforcement or the issuing authority.

[WORKFLOW // ESCALATION]

From interview to investigation

01

Interview passed

Candidate clears the interview process

02

Concern raised

Internal flag about candidate behaviour

03

Verification review

HR re-checks submitted records

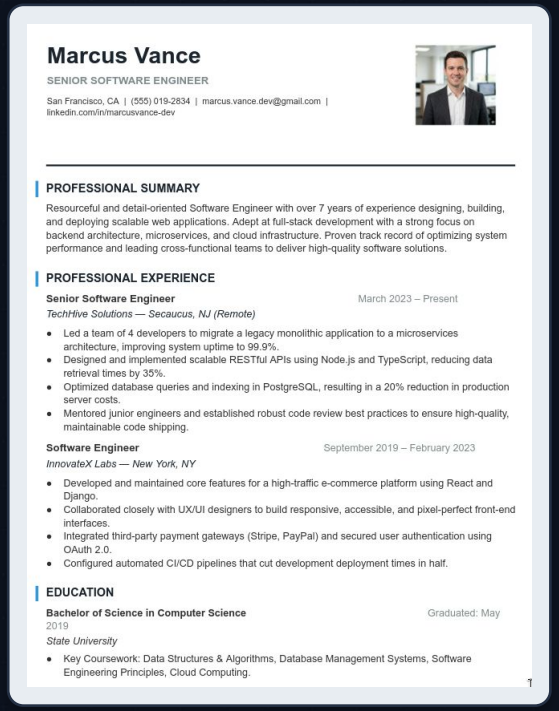
04

Mismatch found

Identity discrepancy in screening docs

[CASE FILE // RESUME]

Catching a ghost with a resume



Marcus Vance

SENIOR SOFTWARE ENGINEER

San Francisco, CA | (555) 019-2834 | marcus.vance.dev@gmail.com | linkedin.com/in/marcusvance-dev

PROFESSIONAL SUMMARY

Resourceful and detail-oriented Software Engineer with over 7 years of experience designing, building, and deploying scalable web applications. Adept at full-stack development with a strong focus on backend architecture, microservices, and cloud infrastructure. Proven track record of optimizing system performance and leading cross-functional teams to deliver high-quality software solutions.

PROFESSIONAL EXPERIENCE

Senior Software Engineer March 2023 – Present

TechHive Solutions — Secaucus, NJ (Remote)

- Led a team of 4 developers to migrate a legacy monolithic application to a microservices architecture, improving system uptime to 99.9%.
- Designed and implemented scalable RESTful APIs using Node.js and TypeScript, reducing data retrieval times by 35%.
- Optimized database queries and indexing in PostgreSQL, resulting in a 20% reduction in production server costs.
- Mentored junior engineers and established robust code review best practices to ensure high-quality, maintainable code shipping.

Software Engineer September 2019 – February 2023

InnovateX Labs — New York, NY

- Developed and maintained core features for a high-traffic e-commerce platform using React and Django.
- Collaborated closely with UX/UI designers to build responsive, accessible, and pixel-perfect front-end interfaces.
- Integrated third-party payment gateways (Stripe, PayPal) and secured user authentication using OAuth 2.0.
- Configured automated CI/CD pipelines that cut development deployment times in half.

EDUCATION

Bachelor of Science in Computer Science Graduated: May 2019

State University

- Key Coursework: Data Structures & Algorithms, Database Management Systems, Software Engineering Principles, Cloud Computing.

THE GIVEAWAY

Same photo. Different name.

Reverse image search exposed a single operator behind multiple personas.

[LEGAL // USA 🇺🇸]

What is actually allowed?

LEGAL FRAMEWORKS

§ FCRA + CA ICRAA

Third-party background checks need standalone written disclosure + consent. Adverse action needs pre- and post-notice. California's ICRAA layers on stricter state-level disclosure & consent for investigative reports.

Anti-Discrimination Laws

Title VII/EEOC — no disparate impact on protected classes; risk of liability.

Off-duty conduct — "lawful activities" laws (CA, CO, NY) protect legal off-duty conduct.

Social media & privacy — SCA/CFAA bar bypassing privacy settings to view profiles.

Ban-the-Box & State Laws

37 states + 150+ localities
limit when you can ask about criminal history

22 states
ban salary-history questions. Rules vary.

GDPR & AUTOMATED SCREENING

GDPR — screening an EU-based candidate

Lawful basis — a defined legal ground to process at all

Data minimization — collect only what the role requires

Transparency & erasure — disclose what's collected; candidates can request or delete it

Automated screening (AI): NYC LL144, Colorado's AI Act & the EU AI Act layer bias-audit and disclosure duties on top of anti-discrimination law — AI doesn't excuse you from it.

YOU CAN

- ✓ Check professional networks (LinkedIn)
- ✓ Verify credentials directly with issuers
- ✓ Use reverse image search
- ✓ Run FCRA-compliant checks with consent
- ✓ Follow adverse-action steps & document

YOU CANNOT

- ✗ Access breach data directly
- ✗ Skip FCRA disclosure or consent
- ✗ Use blanket criminal-history exclusions
- ✗ Ask salary history where it's banned

Informational purposes only — not legal advice.

[PLAYBOOK // CHECKLIST]

Pre-employment verification checklist

Practical steps HR & security teams can implement today

1. **Reverse-image all photos**
   Run profile images through Google, TinEye, PimEyes.
2. **Cross-reference locations**
   Resume vs LinkedIn vs shipping — addresses must match.
3. **Analyse resume language**
   Stylometric overlap with other CVs signals templated fraud.
4. **Check contact details**
   Shared phone / email / address across applicants is a red flag.
5. **Username enumeration**
   Maigret / Sherlock — check account age & genuine activity.
6. **Verify credentials at source**
   Contact universities & licensing bodies directly.
7. **Analyse video interviews**
   Watch for deepfake artefacts, lighting & audio-sync issues.
8. **Ship to verified addresses**
   Require ID at pickup — KnowBe4 now ships to UPS stores.

⚠ **Remember:** document your lawful basis first, and run checks only on selected candidates — not every applicant.

[DEFENSE // OPSEC]

Flip the script: protect yourself

Digital hygiene to reduce your own OSINT exposure

PLATFORM SETTINGS

LinkedIn

Disable public profile, hide connections

Facebook

Friends-only, restrict old posts, no lookups

Twitter / X

Protect posts, disable discoverability

OPT-OUT PRIORITIES

UK Electoral Roll

Opt out of the Open Register

Companies House

Use a registered office; SR01 form

192.com

Submit a C01 form for removal

COMPARTMENTALISE

Usernames

Never reuse handles across platforms

Email aliasing

SimpleLogin / AnonAddy per service

Photo metadata

Strip EXIF — GPS reveals your home

[SUMMARY // TAKEAWAYS]

Key takeaways

1

Background checks aren’t enough

They verify documents, not identity. OSINT catches fabricated personas.

2

Reverse image search is mandatory

Stock & AI photos are the top indicator of identity fraud in remote hiring.

3

Document your lawful basis first

Legitimate interest works but needs an LIA. Never access breach data.

4

Apply OSINT to yourself

Opt out of data brokers, compartmentalise usernames, audit quarterly.

[REFERENCE // USA 🇺🇸]

Tools quick reference

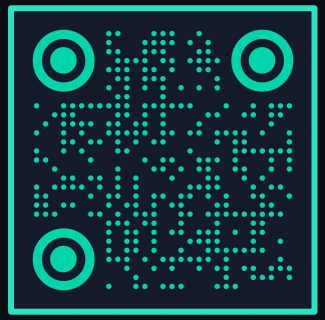
CATEGORY	TOOL	NOTES	COST
Username	**OSINT Industries**	Real-time lookup of accounts linked to emails or phones	Free / $25–125/mo
Facial	**PimEyes**	2.1B faces · Bellingcat-approved · includes takedown help	$30–90/mo
Facial	**FaceCheck.ID**	700M+ faces incl. mugshots · confidence scores 50–100	Pay-per-use
Email	**holehe / Epieos**	120+ sites via password reset · doesn't alert target	Free
Email	**GHunt**	Analyse Google accounts for linked public activity	Free
Phone	**PhoneInfoga**	Carrier lookup, VoIP detection, porting history	Free
Metadata	**ExifTool / FOCA**	GPS, device info, author names from 200+ file types	Free
Framework	**Maltego / SpiderFoot**	Visual link analysis · 200+ data sources	Free / $999+
Web	**Wayback Machine**	Verify past employment on archived company pages	Free
Breach	**Have I Been Pwned**	2B+ emails · shows registrations via breach dates	Free
Username	**Maigret / Sherlock**	3,000+ sites · ~30% false positives — always verify	Free

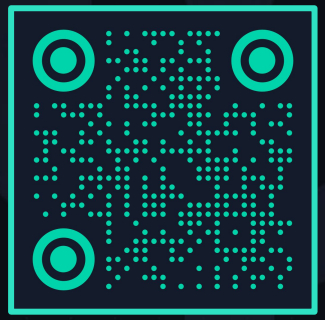
⚠️ Pipl is now enterprise-only — no consumer searches. ⚠️ Clearview AI is law-enforcement only.

END OF BRIEFING

Q&A

Thank you for listening.





RISHI Senior Security Researcher

MICHAEL Product Security