

2025 Report

The invisible workforce

How fake identities, “interview farms,” and AI-powered fraud are infiltrating critical infrastructure



The Invisible Workforce

How Fake Identities, Interview Farms, and AI-Powered Deception Are Infiltrating Global Companies

A Critical Threat Assessment for Enterprise Leaders

November 2025

Contents

The Invisible Workforce	2
Executive Summary	3
A Personal Reflection on an Emerging Threat	4
The Problem: A Global Employment Fraud Crisis	6
The Technology Enabling the Threat	9
Case Studies: The Threat in Practice	10
Business Impact and Consequences	16
The European Dimension: A Growing Target	18
The Human Firewall: Why Background Screening is Your First Line of Defense . . .	20
European Regulatory Response: CER Directive and National Implementation	29
Detection and Prevention Strategies	31
Red Flags During Recruitment	31
Strategic Recommendations	35
Scout: Your Partner in Secure Hiring	37
Sources and Citations	40
Conclusion: The Urgency of Action	43
About This Report	45

Executive Summary

A sophisticated, state-sponsored employment fraud operation has evolved from a nascent threat into a global crisis affecting Fortune 500 companies, government contractors, healthcare organizations, and technology firms worldwide. What began as isolated incidents has exploded into an industrial-scale infiltration campaign, with threat actors using advanced AI, deepfake technology, and organized crime syndicate tactics to embed fraudulent workers into legitimate organizations.

Key Findings:

- Criminal organizations have generated over \$17 million through a single laptop farm operation involving 309 fraudulent hires across U.S. companies
- Deepfake technology can now be created in under 70 minutes with no specialized skills, using consumer-grade hardware and freely available tools
- Nearly every Fortune 500 CISO has encountered this threat within their organization, according to Mandiant CTO
- The threat has expanded beyond North America, with organized operations now active in Europe (Germany, Portugal, Poland, Romania, UK), Russia, and Asia
- 27% of identified fraudulent IT worker interviews now target non-U.S. companies
- Interview farms in Asia enable real-time impersonation, with teams conducting hundreds of simultaneous job interviews using fake identities
- 85 healthcare organization interviews detected in 2025 alone, providing potential access to sensitive patient data

220%

Increase in North Korean IT worker infiltrations over 12 months

1 in 4

*Candidate profiles will be fake by 2028
(Gartner prediction, July 2025)*

The threat extends beyond mere employment fraud. Once embedded, these operatives engage in intellectual property theft, ransomware deployment, espionage, and data exfiltration. Some have transitioned to extortion, threatening to release stolen proprietary information unless paid. The traditional security perimeter has been breached—the threat actor is already inside, working alongside legitimate employees, with full network access and trusted credentials.

This white paper provides a comprehensive analysis of this evolving threat, examining the operational infrastructure, attack methodologies, real-world impact, and defensive

strategies. Most critically, it addresses a gap that many organizations have failed to recognize: HR departments and recruiters do not own cybersecurity risk, creating a dangerous blind spot in organizational defenses.

The threat of unintentionally hiring North Korean IT workers is larger than most people realize. It is covert, it is global, and it is active right now.

— Kevin Mandia, Former CEO of Mandiant

A Personal Reflection on an Emerging Threat

In 2020, as the world grappled with the unprecedented challenges of the COVID-19 pandemic, my team at Scout.com—a nascent venture dedicated to advanced background screening—stumbled upon early indicators of a sophisticated fraud operation linked to North Korean hackers. What began as isolated anomalies in candidate verifications soon revealed a pattern of deceptive identities and coordinated infiltration tactics. Little did we anticipate that, five years on, this threat would balloon to an industrial scale, ensnaring Fortune 500 companies, healthcare providers, and critical infrastructure worldwide.

Equally startling is the persistent gap in awareness: even now, only a minority of recruiters and HR professionals are attuned to these risks, allowing the schemes to proliferate unchecked. This realization compelled us to marshal every resource at our disposal—not merely as a business imperative, but as a duty to the broader community—to disseminate this intelligence, chronicle the full scope of the operation, and equip organizations with the tools to safeguard against its escalation.



As the CEO and founder of Scaut.com, a provider of automated background screening solutions based in Prague, Czech Republic, I have witnessed firsthand the evolution of cybersecurity threats intertwined with human resource vulnerabilities. Established in 2020, Scaut was conceived to address the growing need for precise, compliant verifications in an increasingly remote and globalized workforce. Our SaaS platform, which integrates cutting-edge technology with rigorous analyst oversight, enables companies to conduct comprehensive checks—from identity validation and criminal records to sanctions screening and ongoing monitoring—ensuring trust and regulatory adherence across supply chains.

The discovery of North Korean-linked fraud in our inaugural year was serendipitous yet alarming. Amid the global fixation on public health crises, our systems flagged inconsistencies in applicant data that traced back to state-sponsored actors employing fake identities, interview farms, and AI-driven deceptions. Reports from that period, corroborated by subsequent analyses, indicated these operatives were embedding themselves in Western firms to siphon salaries and intellectual property, funding regime activities while evading sanctions.

By 2025, as detailed in our own publications and echoed in industry reports, the scale has intensified: infiltrations have surged, with documented cases generating millions in illicit gains through mechanisms like U.S.-based laptop farms. Yet, the most disconcerting aspect is the inertia in response. Surveys and expert insights reveal that, despite high-profile breaches and warnings from entities like the FBI and ENISA, a significant portion of (European) recruitment professionals remain unaware or underprepared.

This blind spot—often stemming from siloed HR and security functions—exposes organizations to insider threats, data exfiltration, and reputational harm. At Scaut, this disparity galvanized our mission: we became the first European screening firm to publicly highlight these infiltrations, developing specialized tools to detect anomalies such as IP mismatches, scripted interview responses, and fabricated credentials.

Our commitment extends beyond awareness to actionable solutions. Scaut's platform offers a tiered structure tailored to diverse needs, from pay-as-you-go basics to enterprise-grade subscriptions with advanced features and custom workflows. Compliance is foundational: we hold ISO 27001 certification and employ end-to-end encryption, ensuring GDPR adherence while minimizing data exposure. This white paper represents our contribution to the collective defense—a comprehensive threat assessment combined with practical countermeasures.



The Problem: A Global Employment Fraud Crisis

The Scope of Infiltration

What was once dismissed as an isolated curiosity has metastasized into an industrial-scale operation. State-sponsored actors, primarily from the Democratic People's Republic of Korea (DPRK), have built a sophisticated employment fraud ecosystem that combines traditional identity theft, advanced technology, and organized crime methodologies.

Between 2021 and mid-2025, identity verification firm Okta tracked more than 130 confirmed fraudulent identities conducting over 6,500 initial job interviews across more than 5,000 different companies worldwide. However, this represents only the tip of the iceberg—these are merely the cases that were detected and documented. The true scale is likely exponentially larger.

Recent reporting reveals alarming growth trajectories:

- CrowdStrike investigators observe approximately one North Korean IT worker incident per day
- Infiltrations increased 220% over a 12-month period through mid-2025
- Thousands of operatives have successfully infiltrated Fortune 500 companies
- A single Arizona laptop farm operation generated \$17.1 million in illicit revenue through 309 fraudulent hires

The Criminal Infrastructure

This is not the work of isolated individuals. The DPRK has constructed a comprehensive criminal enterprise that functions more like a state-sponsored mafia than a traditional intelligence operation. The system involves multiple specialized roles and sophisticated logistics:

Identity Theft and Fabrication

Operatives begin by acquiring or creating false identities. Some steal legitimate identities from real individuals through data breaches or social engineering. Others fabricate entirely synthetic identities using AI-powered tools. Services like Verif Tools generate convincing fake identity documents—passports, national ID cards, bank statements, university diplomas—for as little as \$8.99. These documents are digital photographs designed to pass scrutiny in online verification processes.

Interview Farms

In India, Pakistan, China, and other Asian locations, specialized facilities have emerged where dozens of operators conduct simultaneous job interviews. For \$200-500 per interview, candidates receive comprehensive support: someone listens to questions and provides answers via ChatGPT, another person handles technical coding tests, and a third manages screen sharing and documentation. The actual candidate becomes merely a face on camera while a team operates behind the scenes. Just google the term “Interview Support Proxy Facebook” and you will find numerous groups...

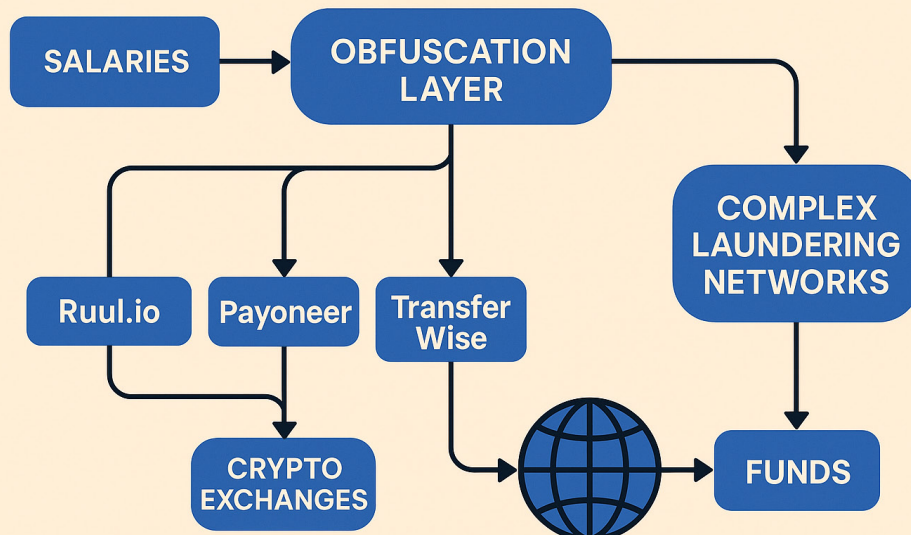
U.S. and European Facilitators

The operation requires accomplices in target countries. These facilitators—some witting, many unwitting—provide critical services: receiving company laptops and installing remote access software, establishing financial accounts, creating business addresses, purchasing AI tools and background check services, and even attending virtual interviews on behalf of North Korean workers. One Arizona woman, Christina Chapman, received an 8.5-year prison sentence for operating a laptop farm that maintained 90 laptops and facilitated 309 fraudulent hires generating \$17.1 million.

Payment Obfuscation

Salaries flow through complex money laundering networks. Payment platforms like Ruul.io, Payoneer, TransferWise, and cryptocurrency exchanges serve as intermediaries—often unknowingly. These legitimate businesses become unwitting participants in sanctions evasion, as funds ultimately route to DPRK government accounts. The operatives frequently change bank accounts as institutions close suspicious accounts, creating a constant cat-and-mouse game.

PAYMENT OBFUSCATION

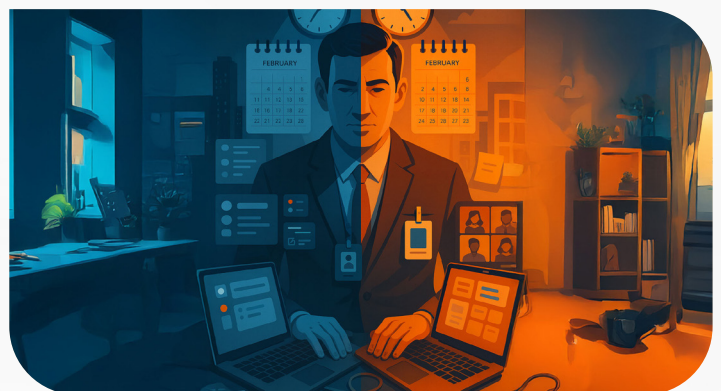


DPRK Organizational Structure and Motivations:

Research from DTEX Systems reveals that DPRK operations function as a survival-driven crime syndicate, not merely traditional state espionage. The regime operates a sophisticated organizational hierarchy that blurs lines between cybercrime, espionage, and military operations. Operatives are motivated by basic survival needs—food, education for their families, and escape from crushing poverty—within North Korea’s scarcity economy. This creates extraordinarily motivated threat actors who combine desperation with elite technical training.

Key organizational elements include:

1. **Research Center 227:** An advanced AI development hub responsible for creating deepfake technology, autonomous systems, and high-velocity operations. This center accelerates the production of fake identities and enables operatives to conduct convincing video interviews using AI-generated personas.
2. **RGB (Reconnaissance General Bureau):** The primary intelligence and special operations agency, responsible for foreign intelligence collection, cyber operations, and sabotage. RGB units frequently share resources with employment fraud operations, creating fluid connections between hiring scams and broader espionage campaigns.
3. **Talent Pipeline:** The DPRK identifies technically gifted children as young as age 10 and funnels them into elite training programs. Graduates receive advanced education in mathematics, computer science, and foreign languages before deployment to overseas operations. This produces extraordinarily capable infiltrators with genuine technical expertise.
4. **Multi-Job Strategy:** Many operatives simultaneously hold multiple full-time positions, using AI tools to manage communications, automate routine tasks, and maintain the illusion of dedicated single employment. This maximizes revenue extraction while maintaining cover.



Understanding this organizational structure is critical for defenders. These are not amateur scammers or isolated opportunists—they are products of a decades-long state program specifically designed to infiltrate Western technology companies and critical infrastructure. The regime generates an estimated \$1 billion annually through cryptocurrency theft and employment fraud, with funds directly financing weapons development programs. Every fraudulent hire contributes to nuclear proliferation and destabilization campaigns.

The Technology Enabling the Threat

Deepfakes: From Science Fiction to Commodity

In April 2025, Unit 42 researchers at Palo Alto Networks conducted an experiment: could someone with no technical expertise create a convincing deepfake for use in a job interview? The answer was startling. Using only an AI search engine, a five-year-old consumer laptop with a GTX 3070 graphics card, and freely available tools, they created a functional real-time deepfake in just over 70 minutes.

This represents a fundamental shift in threat dynamics. What once required specialized knowledge, expensive equipment, and significant time investment is now accessible to anyone. The technology has become democratized, and the DPRK has capitalized on this accessibility.

How the technology works:

- Operatives use face-swapping applications to replace their appearance with synthetic faces generated by tools like ThisPersonDoesNotExist.com
- Real-time video processing allows instant facial manipulation during live video calls
- Voice modulation and real-time translation tools mask accents and language barriers
- AI assistants provide instant answers to technical questions, creating the illusion of deep expertise
- Multiple monitors allow operators to view questions, reference materials, and manage their synthetic persona simultaneously

CrowdStrike has documented North Korean operatives actively searching for and subscribing to premium deepfake services during operations. The investment is minimal—often less than \$50 per month—but the return on investment is extraordinary when a single fraudulent hire can generate \$100,000 or more in annual salary.

AI-Powered Identity Construction

Generative AI has transformed every stage of the fraud lifecycle. Okta researchers documented extensive use of AI tools throughout the operation:

During Job Application:

- AI generates compelling resumes and cover letters tailored to specific job descriptions
- Tools optimize applications to bypass automated CV scanning systems
- Synthetic profiles on LinkedIn combine AI-generated photos with fabricated career histories
- Background images for fake identity documents are generated using Midjourney or DALL-E

During Interviews:

- Real-time translation services enable non-native English speakers to communicate fluently
- Mock interview services provide practice and feedback to improve performance
- AI evaluates deepfake video quality and suggests lighting improvements
- Chatbots provide instant answers to technical questions

Post-Employment:

- AI helps maintain multiple simultaneous jobs by assisting with Slack communications and email responses
- Code generation tools enable workers to meet deliverables despite limited actual expertise
- Language processing ensures grammatically correct, professionally written communications

Case Studies: The Threat in Practice

Case Study 1: The Czech Cloud Company (2023)

In 2023, a Czech cloud services company posted a software developer position on LinkedIn. Among the applicants was Denys Emil L., claiming Danish citizenship and residence. His profile appeared professional: Asian appearance, legitimate-looking credentials, proper documentation. He passed initial HR screening and submitted identity documents including passport and previous work history statements.

However, Scout, who was tasked by running a background check on the candidate detected anomalies. One of our analysts discovered that Denys's identity documents had been generated using online tools. His other documents were indistinguishable fakes. He had borrowed an identity of an unknowing Danish citizen - whose trade license registration he was attempting to use for the fraud. Investigation revealed that Denys Emil was actually a Chinese citizen who had created multiple false identities to apply for positions across Western companies. This was not an isolated attempt—he was systematically targeting multiple employers simultaneously.

The case raises critical questions: Was this industrial espionage, an attempt to access proprietary cloud infrastructure? Was it part of a larger employment fraud ring? The investigation would later tie the attacker to an organized group with ties to North Korea. The operation and systematic targeting of technology companies suggests state-sponsored coordination rather than individual fraud.

Case Study 2: KnowBe4 Security Firm (2024)

Perhaps most embarrassingly, KnowBe4—a cybersecurity awareness training company—inadvertently hired a North Korean IT worker. The individual passed background checks, conducted professional interviews, and received a company laptop. Upon receiving the device, the operative immediately began attempting to load malware onto the corporate workstation.

KnowBe4's security team detected the suspicious activity and terminated the employment. The company publicly disclosed the incident in a detailed blog post, providing a valuable case study of the threat. If a company specializing in security awareness can fall victim, any organization is vulnerable.



Case Study 3: Chapman Laptop Farm (2024-2025)

Christina Chapman, a 50-year-old Arizona resident, operated what prosecutors called a laptop farm from her home. She received and maintained 90 company-issued laptops on behalf of North Korean IT workers, installing remote access software that allowed operatives overseas to work as if physically located in the United States.

The operation was extraordinarily successful: 309 fraudulent hires across U.S. companies generating \$17.1 million in revenue. Nearly 70 Americans had their identities stolen to facilitate the scheme. Victims included major corporations—Nike confirmed in a victim impact statement that it had unwittingly employed a North Korean operative through Chapman's operation.

Chapman pleaded guilty and received an 8.5-year prison sentence. However, authorities believe her operation was just one of many. CrowdStrike reports that laptop farms have now been established in Western Europe, particularly Romania and Poland, replicating the model as U.S. law enforcement crackdowns made domestic operations more difficult.



Case Study 4: European Interview Farm Operations (2024-2025)

A Czech IT recruitment professional with experience conducting hundreds of interviews reported an alarming pattern emerging over the past two years. Candidates with perfect resumes, professional LinkedIn profiles, and excellent written communication skills would join video calls with consistent red flags:

- Cameras frequently malfunctioning or disabled
- Multiple voices audible in the background, suggesting call center environments
- Answers to technical questions flowing smoothly, but personal questions causing hesitation
- Requests for clarification about background noise met with immediate disconnection
- IP addresses revealing Asian locations despite claims of European residence

Investigation revealed these candidates were calling from Asian interview farms—facilities where teams of operators assist dozens of job applicants simultaneously. The scale suggests industrial organization rather than individual attempts. When confronted with specific questions about their claimed location or asked to point their camera out a window, candidates would immediately terminate the call. In nine out of ten such incidents, the candidate never responded to follow-up communication.

Case Study 5: German Energy Infrastructure Company (2024)

A major German energy infrastructure operator, classified as critical infrastructure under both German KRITIS regulations and the EU's Critical Entities Resilience (CER) Directive, discovered a sophisticated infiltration attempt during a routine security audit in late 2024. The company had hired what appeared to be a highly qualified systems engineer with German credentials and extensive experience in SCADA systems management.

The operative had successfully passed initial screening and worked for three months managing critical energy distribution systems before anomalies were detected. Security teams noticed unusual network traffic patterns: data exfiltration attempts targeting industrial control system configurations, grid topology maps, and operational protocols. Further investigation revealed the employee was using remote access software to allow someone in Asia to control his workstation during off-hours.

The breach represented a catastrophic security failure with potential national security implications. The operative had access to systems controlling power distribution for hundreds of thousands of households and industrial facilities. German authorities classified the incident as a state-sponsored espionage operation, though the company's name was not publicly disclosed to prevent reputational damage. The case accelerated discussions about mandatory personnel security screening for critical infrastructure operators across the EU.

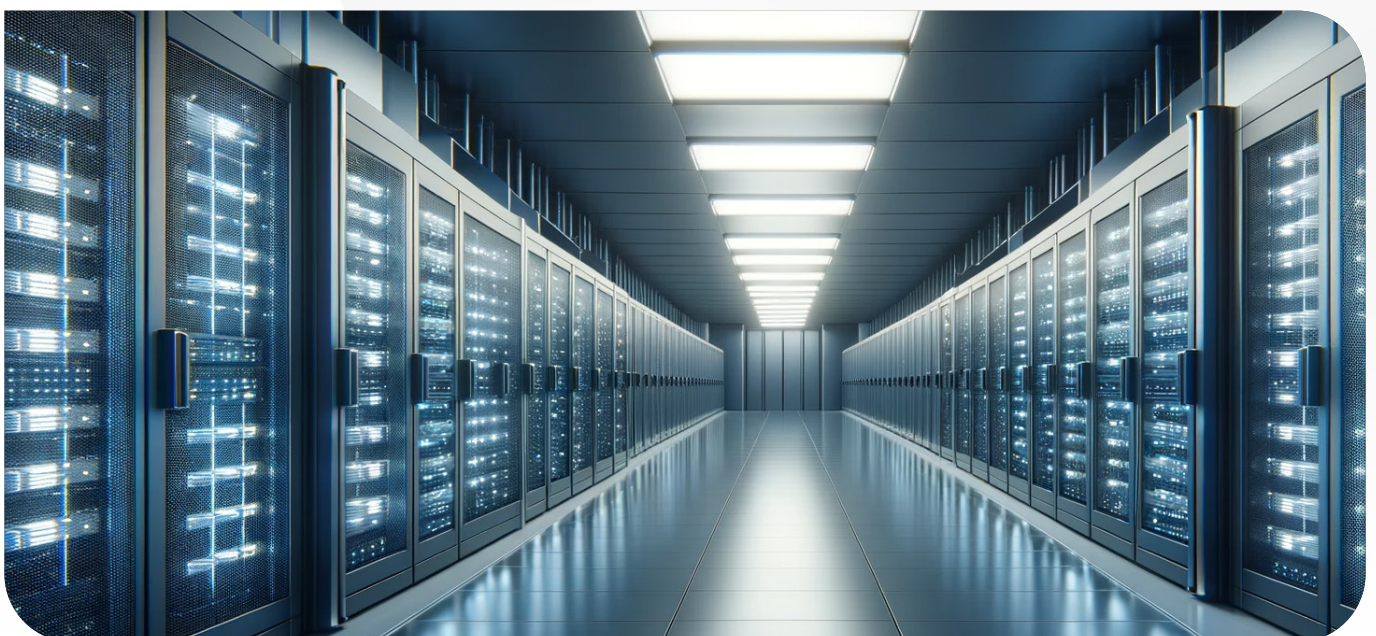
Case Study 6: UK Healthcare Data Breach (2025)

In early 2025, a UK National Health Service (NHS) contractor discovered that a database administrator hired six months earlier had exfiltrated over 4.2 million patient records. The operative, claiming British citizenship and presenting flawless documentation, had been granted privileged access to healthcare databases containing sensitive medical histories, treatment records, and personal identifiable information.

The incident involved Synnovis, a pathology services provider serving major London hospitals, and the breach directly contributed to a subsequent ransomware attack that disrupted services across multiple NHS facilities, demonstrating how personnel security failures can cascade into broader operational crises.

Detection occurred when an automated system flagged unusual bulk data exports occurring during weekend hours when the employee was supposedly offline. Forensic analysis revealed the operative had systematically copied entire database tables to encrypted external storage over several months. The exfiltrated data included not only standard medical records but also mental health assessments, substance abuse treatment histories, and genetic testing results—precisely the type of sensitive information valuable for blackmail, insurance fraud, and identity theft operations.

The breach cost exceeded £22 million in immediate response, notification, credit monitoring services, and regulatory fines under UK GDPR. More significantly, it triggered a comprehensive review of contractor vetting procedures across the NHS. The Information Commissioner's Office (ICO) cited inadequate employee screening as a contributing factor, noting that the contractor had failed to verify the operative's claimed work history and educational credentials. The case became a reference point in UK policy discussions about healthcare sector security requirements.



Case Study 7: Polish Financial Institution Payment Diversion (2024)

A Warsaw-based financial services company discovered in mid-2024 that a senior software developer had orchestrated a sophisticated payment diversion scheme. The operative, who had worked for the company for nearly eight months, had embedded malicious code into the payment processing system that redirected small amounts from international wire transfers to cryptocurrency accounts.

The scheme was remarkably subtle: the malicious code rounded down transaction amounts by fractions of a cent, diverting the difference to external accounts. Over eight months, the operation siphoned approximately €840,000 before being detected during a routine audit. The operative had presented Polish citizenship documents and claimed previous employment at legitimate financial institutions in Estonia and Lithuania. Background verification later revealed all documentation was fabricated using AI-generated identity documents.

What made this case particularly concerning was the operative's technical sophistication and patience. Rather than conducting an obvious smash-and-grab attack, the scheme was designed for long-term exploitation and went undetected for months. Polish financial regulators used the incident to advocate for enhanced personnel security requirements in the financial sector, particularly for roles with access to payment systems and core banking infrastructure. The case also highlighted the vulnerability of Eastern European financial institutions, which face particular targeting due to their proximity to hostile actors and their role as gateways to the broader European financial system.

Case Study 8: Trust as the Target (2025)

In early 2025, an Austrian company—an international leader in wastewater treatment—found itself under quiet but intense investigation. The reason wasn't a data breach, a ransomware attack, or a stolen password. It was a person.

A suspected Russian agent had allegedly embedded themselves within the organization—not by hacking their way in, but by befriending a senior engineer. There were no shadowy night intrusions or digital fingerprints of intrusion. The agent attended seminars, joined technical discussions, shook hands, exchanged ideas, and over time became part of the trusted circle. For years, they went unnoticed. This case became a pivotal lesson for Europe's industrial and security community. The intrusion was not into a server room but into the human layer of the organization—the social graph of trust that underpins modern business.

The message was unmistakable: knowing your employees is not enough. You must understand who they know, and who's being allowed into your orbit under the banner of "collaboration." The investigation exposed a crucial vulnerability: external trust. Contractors, visiting experts, seminar attendees—all can become nodes of access.

Because when an outsider can sit in your meeting as a “friend of a colleague,” or wander your facilities as a “visiting professional,” the strength of your cybersecurity architecture becomes irrelevant.

The most valuable asset in any organization isn’t technology—it’s trust. And the weakest link isn’t a password. It’s the person you trusted without verifying.

The Austrian case should serve as a wake-up call across Europe’s critical infrastructure sectors, demonstrating that infiltration today looks nothing like espionage of the past. It doesn’t break in—it’s invited.

Business Impact and Consequences

Financial Costs

The direct financial impact of this threat extends across multiple dimensions:

Salary Theft and Revenue Generation:

Each fraudulent hire generates \$50,000-150,000 in annual salary, with funds ultimately flowing to the DPRK regime. The Chapman operation alone generated \$17.1 million. With thousands of such operatives employed globally, the total annual revenue likely exceeds \$100 million, directly funding weapons development and sanctions evasion.

Operational Inefficiency:

Many fraudulent workers hold multiple simultaneous positions, dividing attention and delivering substandard work. Companies pay full-time salaries for part-time effort, experiencing project delays, quality issues, and technical debt. The cost of remediation—rewriting poor code, fixing security vulnerabilities, recovering from project failures—often exceeds the original salary expense.

Data Breach and Intellectual Property Theft:

According to IBM’s 2024 Cost of Data Breach Report, the average cost of a data breach globally is \$4.88 million. Healthcare breaches average \$11 million. When operatives exfiltrate proprietary source code, customer data, or strategic information, the financial impact can be catastrophic. The value of stolen intellectual property in technology, finance, and healthcare sectors is incalculable.

Ransomware and Extortion:

Since late 2024, an increasing number of operatives have transitioned to extortion after termination. Secureworks documented cases where recently fired IT workers threatened to release proprietary data or provide it to competitors unless paid. This represents evolution from passive data theft to active monetization, significantly escalating the threat.

Regulatory and Legal Exposure

Organizations that unknowingly employ DPRK operatives face severe legal consequences:

Sanctions Violations:

Payments to North Korean nationals violate U.S., EU, and U.N. sanctions. Even inadvertent violations can result in significant penalties. U.S. companies face potential Office of Foreign Assets Control (OFAC) enforcement actions, with fines ranging from hundreds of thousands to millions of dollars.

Data Protection Violations:

Under GDPR, NIS2, CER, and similar regulations, organizations have strict obligations to protect personal and sensitive data. If a fraudulent worker exfiltrates customer information, the company faces potential fines of up to 4% of global annual revenue under GDPR. Healthcare organizations in the U.S. face HIPAA penalties. Financial institutions risk regulatory sanctions from their primary regulators.

Shareholder and Customer Lawsuits:

Following data breaches or security incidents, companies face class-action lawsuits from affected customers and shareholder derivative suits alleging inadequate security controls. The reputational damage can exceed direct financial costs, as customers lose trust and investors question governance.



The European Dimension: A Growing Target

Geographic Expansion Beyond North America

As U.S. law enforcement has intensified crackdowns—including indictments, laptop farm disruptions, and public awareness campaigns—DPRK operations have deliberately diversified geographically. Google's Threat Intelligence Group reports confirmed expansion into multiple European countries:

Currently, 27% of identified fraudulent IT worker interviews target non-U.S. companies. CrowdStrike reports investigating European incidents daily. The UK Treasury's Probability Yardstick assessment indicates with almost certainty that fake IT workers have targeted UK businesses.



Why Europe Is Vulnerable

Fragmented Regulatory Environment:

Unlike the U.S., where FBI warnings and federal coordination create unified awareness, Europe's 27 member states operate with varying levels of cyber maturity and different enforcement priorities. While NIS2 attempts harmonization, implementation remains inconsistent. Many European organizations lack awareness of the threat entirely.

Bureaucratic Complexity:

European hiring processes often involve extensive paperwork, multiple approvals, and lengthy timelines. According to the World Bank's Ease of Doing Business index, many European countries rank below Asian and North American peers in administrative efficiency. This complexity paradoxically creates shortcuts: overwhelmed HR teams may reduce verification rigor to accelerate hiring, creating exploitable gaps.

Remote Work Normalization:

COVID-19 permanently normalized remote work in Europe. Many technology companies now embrace fully distributed teams, never meeting employees in person. The cultural shift toward trust-based remote work has inadvertently lowered verification standards.

Lack of Ownership:

In European organizations, no single entity typically owns this risk. HR departments focus on candidate experience and speed-to-hire, not counterintelligence. Security teams focus on network defense, not employee verification. Legal and compliance teams focus on GDPR and NIS2, not employment fraud. The result: a dangerous blind spot where no one takes responsibility for preventing infiltration.



The Human Firewall: Why Background Screening is Your First Line of Defense

A Personal Perspective from Petr Moroz, CEO and Founder, Scout.com

When we discovered our first suspected North Korean operative in 2020, I remember the moment vividly. It wasn't a sophisticated AI algorithm that caught him. It wasn't an automated fraud detection system or a blockchain-verified identity platform. It was Anna, one of our senior analysts, who paused mid-review and said: "Something doesn't feel right about this candidate."

The documents looked perfect—too perfect, actually. An Estonian passport with all the right security features - even a QR code leading to governmental confirmation of authenticity. University transcripts from a respected technical school. Everything checked out on the surface. But Anna noticed something subtle: the candidate's LinkedIn profile picture, which was clearly a stock image. Later we discovered multiple profiles with slight misalignments in data. His professional references were way too fast to answer - as if they were expecting us, however couldn't recall specific project details when pressed for follow-up. His email communication patterns suggested someone operating in an Asian time zone despite claiming European residence.

These weren't data points that triggered algorithmic red flags. They were signals that required human interpretation—the ability to synthesize disparate pieces of information, recognize patterns that don't quite align, and ask the questions that machines don't know to ask. This is what I call the human firewall: the critical layer of intelligent human analysis that stands between raw data and informed hiring decisions.



The Myth of Automated Security

In cybersecurity, we've built remarkable technological defenses. Firewalls that monitor billions of packets per second. Intrusion detection systems powered by machine learning. Zero-trust architectures that verify every access request. Yet here's the paradox: **the most sophisticated threat actors don't break through your firewall—they walk through your front door with a job offer letter and a company laptop.**

Traditional security focuses on the perimeter: keeping unauthorized actors out of your network. But what happens when the threat actor is authorized? When they have valid credentials, approved system access, and a legitimate employment contract? Your intrusion detection system doesn't trigger because there's no intrusion—the person is supposed to be there. Your data loss prevention tools don't alert because the employee has appropriate clearance to access the information they're exfiltrating.

This is where the human firewall becomes essential. Background screening isn't just an HR compliance checkbox—it's the first and often most critical line of defense against insider threats that bypass every other security control you've invested in. It's the difference between discovering a fraudulent employee during the hiring process versus discovering them six months later when they've already stolen your intellectual property, installed backdoors in your systems, or sold access to your network to ransomware gangs.

The Three Dimensions of Modern Background Screening

Over the past five years of fighting this threat, I've come to understand that effective background screening operates across three critical dimensions, each requiring both technological capability and human expertise:

1. *Pre-Employment Screening: The Critical Gate*

This is where the battle is won or lost. Once someone receives a company laptop and network credentials, removing them becomes exponentially more difficult and costly. Pre-employment screening is your opportunity to catch threats before they gain access. But here's what most organizations get wrong: they treat it as document verification rather than threat intelligence.

Consider what we discovered about that first operative in 2020. His documents weren't technically fraudulent—they were real documents that had been meticulously generated using identity theft and synthetic identity tools. An automated verification system would have approved him instantly. The passport number was valid. The bank account existed. The university confirmed enrollment records. But our analyst saw the inconsistencies in the story those documents told together.

Effective pre-employment screening means connecting data points across multiple sources and looking for narrative coherence. Does the candidate's claimed work history align with their educational timeline? Do their references provide specific details or generic praise? Does their digital footprint match their stated location and employment? Are there gaps in their history that they're reluctant to explain? These questions require human judgment informed by pattern recognition developed through reviewing thousands of legitimate profiles.

At Scout, we've developed what I call "screening with skepticism." Our analysts don't just verify documents; they actively look for reasons to doubt the narrative. This isn't about unfairly targeting legitimate candidates—it's about recognizing that sophisticated threat actors can produce convincing documentation. The goal isn't perfection; it's raising the cost and complexity for fraudulent candidates until the operation becomes uneconomical.

2. Continuous Employment Monitoring: The Evolving Threat

Here's an uncomfortable truth: passing pre-employment screening doesn't mean someone remains trustworthy throughout their employment. Financial difficulties, personal crises, ideological shifts, or external coercion can transform a legitimate employee into an insider threat. Moreover, sophisticated operatives sometimes establish clean credentials years in advance, waiting for the right opportunity.

Continuous monitoring addresses this reality. In critical infrastructure organizations subject to regulatory frameworks, this isn't optional - it's mandatory. But even organizations without legal obligations should consider the risk calculus: what's the cost of discovering a compromised employee after they've spent six months embedded in your systems versus discovering them proactively.

Effective continuous monitoring combines automated alerts with periodic human review. Sanctions list additions, criminal charges, financial distress indicators, social media behavior changes—these can all signal increased risk. But again, technology alone isn't sufficient. When an employee suddenly appears on a financial watchlist, is it because of identity theft targeting them, legitimate financial difficulty, or involvement in illicit activity? Human analysts interpret context and assess actual risk rather than just flagging alerts.

I think of continuous monitoring as the immune system of organizational security. Pre-employment screening is the skin barrier—the first line that blocks most threats. But some threats evade initial detection or develop after entry. Continuous monitoring circulates through the organization, identifying anomalies and responding before they metastasize into catastrophic breaches.

3. *Extended Workforce and Supply Chain Security: The Forgotten Frontier*

This is where organizations consistently fail, and where threat actors increasingly focus their efforts. Why spend months trying to infiltrate a Fortune 500 company directly when you can get hired by one of their contractors, or suppliers, gain access through the supply chain, and operate with less scrutiny?

Consider the attack surface: Your company employs 500 people. You have rigorous background screening, security training, and continuous monitoring. But you also work with 50 contractors, vendors, and service providers who collectively employ another 5,000 people—many of whom have access to your systems, data, or facilities. How many of those 5,000 individuals have been screened to the same standard as your direct employees?

The Chapman laptop farm case illustrates this vulnerability perfectly. Rather than infiltrating target companies directly, North Korean operatives contracted with staffing agencies and outsourcing firms. These intermediaries had minimal screening requirements and were evaluated primarily on cost and delivery speed. The result: 309 successful placements generating \$17.1 million before detection.

Supply chain security isn't just about verifying the security practices of your vendors—it's about verifying the people those vendors employ. This is now explicitly required under the CER Directive and Czech ZKI law: critical infrastructure operators must verify not only their own workers but also personnel from entities essential to delivering basic services. It's recognition that organizational boundaries are porous and that threats don't respect corporate org charts.



At Scout, we've seen the supply chain become the primary attack vector. When we screen contractor personnel, we find fraudulent candidates at rates 3-4 times higher than when screening direct employees. Why? Because threat actors correctly assess that third-party workers face less scrutiny while often receiving equivalent access. Your human firewall needs to extend beyond your corporate perimeter to your entire extended workforce.

The Art and Science of Sifting Signals

What makes a background screening analyst effective? It's not just access to databases or verification tools—it's the ability to sift through noise and identify meaningful signals. In today's environment, we're drowning in data but starving for insight. A typical screening might involve:

1. Identity documents from multiple jurisdictions, each with different security features and verification procedures
2. Employment history spanning multiple countries and languages
3. Educational credentials from institutions with varying verification processes
4. Criminal record databases that may or may not be complete or current
5. Digital footprints across social media, professional networks, and public records
6. Financial records and credit histories that may be legitimate, stolen, or synthetic
7. Reference interviews that may be genuine, scripted, or completely fabricated

An effective analyst doesn't just check whether each piece of information is valid—they assess whether all the pieces fit together into a coherent narrative. They look for what I call “narrative friction”: the subtle inconsistencies that suggest a constructed identity rather than an authentic life history.



For example, a candidate claims five years of remote work experience but their LinkedIn shows they only started using the platform six months ago. That's narrative friction. A candidate provides a reference who enthusiastically praises their technical skills but can't recall which specific technologies they used on projects. That's narrative friction. A candidate's university confirms graduation, but the timing coincides with visa restrictions that would have made physical attendance impossible. That's narrative friction.

None of these individually proves fraud. Many have innocent explanations. But collectively, they create a pattern that warrants deeper investigation. This is where the human firewall excels: recognizing patterns that automated systems miss because they require contextual understanding and cross-domain knowledge.

The Analyst-Recruiter Partnership: Making Sense of Signals

The human firewall isn't just about stopping threats—it's about enabling informed decisions. Background screening analysts aren't gatekeepers who unilaterally reject candidates; they're intelligence analysts who provide recruiters and hiring managers with the information needed to make risk-informed decisions.

This partnership is critical. Recruiters understand the business need, the role requirements, and the candidate's qualifications. Analysts understand verification methodologies, fraud indicators, and threat patterns. Together, they can distinguish between red flags that indicate genuine threats versus benign anomalies that simply require clarification.

Consider a real scenario we encountered: A candidate for a senior engineering role had an employment gap of eight months. Automated screening flagged this as a concern. A superficial review might have rejected the candidate. But our analyst reached out to the recruiter, who contacted the candidate for clarification. The explanation: the candidate had taken parental leave following the birth of twins, during which they completed an advanced certification program. The candidate provided documentation of both the parental leave and the certification. The gap wasn't a red flag—it was a life event that actually enhanced their qualifications.

Contrast this with another case: A candidate had minor inconsistencies in employment dates—a few weeks' discrepancy between their resume and LinkedIn. Easily explained as innocent record-keeping errors. But when our analyst investigated further, they discovered the candidate had fabricated an entire employment history at a company that had gone out of business, making verification difficult. The minor date inconsistencies were actually evidence of a poorly constructed false identity.

The difference between these cases? Human judgment applied to context. This is what separates effective background screening from checkbox compliance. The goal isn't to reject every candidate with an anomaly—it's to identify which anomalies matter and provide recruiters with the intelligence to make informed decisions.

The Cost of Getting It Wrong

I've spent this chapter advocating for robust background screening, but let's be honest about the stakes. What happens when the human firewall fails? What's the actual cost of hiring a fraudulent employee?

The direct financial cost is quantifiable. The Chapman laptop farm generated \$17.1 million in fraudulent salaries. The UK NHS Synnovis breach cost £22 million. The Polish financial institution lost €840,000. These are documented cases with clear financial impact.

But the indirect costs often exceed the direct losses. Intellectual property theft doesn't have a clear price tag until you see your competitor launch your product design six months after you hired that contractor. Network access sold to ransomware gangs doesn't show up on financial statements until your entire operation is encrypted and you're negotiating a ransom. Backdoors installed by embedded operatives don't cost anything until they're used for a cyberattack that brings down critical infrastructure.

And then there's the regulatory exposure. Under Czech ZKI law, failure to properly screen critical infrastructure workers can result in fines up to 50 million CZK or 1.5% of annual turnover. Under GDPR, failure to protect personal data can cost 4% of global revenue. Under various sanctions regimes, inadvertently employing North Korean nationals can result in massive penalties and criminal prosecution.

The question isn't whether you can afford robust background screening. The question is whether you can afford not to have it. A comprehensive pre-employment screening might cost €200-500 per candidate. Continuous monitoring might add €50-100 per employee annually. Supply chain verification might seem complex and expensive. But compared to the cost of a single successful infiltration? The ROI is overwhelming.

Building Your Human Firewall

So how do organizations build an effective human firewall? Based on five years of fighting this threat, here's what I've learned works:

Invest in Expertise, Not Just Technology

Technology is essential—databases, verification tools, AI-powered fraud detection. But technology without human expertise is just expensive automation. Your screening provider should combine advanced tools with experienced analysts who understand threat patterns, can recognize narrative friction, and know when to escalate concerns. At Scout, we invest heavily in analyst training precisely because the human layer is where real value is created.

Match Screening Depth to Risk Level

Not every position requires the same level of scrutiny. A junior marketing coordinator

without system access needs basic verification. A senior database administrator with access to customer data requires comprehensive screening including direct education verification, thorough employment checks, and potentially even financial background review. Critical infrastructure roles under ZKI regulations require minimum standards by law. Risk-based screening allocates resources efficiently while ensuring adequate protection.

Don't Forget the Extended Workforce

Your security is only as strong as your weakest link, and that link is often in your supply chain. Establish screening requirements for contractors, vendors, and service providers. Make background verification a contractual obligation. Audit compliance periodically. The marginal cost of extending screening to your supply chain is minimal compared to the risk reduction.

Implement Continuous Monitoring Where It Matters

You don't need to continuously monitor every employee, but you should monitor anyone with privileged access, financial authority, or exposure to sensitive data. Modern platforms make this cost-effective and minimally intrusive. The goal isn't surveillance—it's early warning of risk factors that require attention.

Foster the Analyst-Recruiter Partnership

Background screening shouldn't be a black box where candidates go in and verdicts come out. Encourage dialogue between screening analysts and hiring teams. When concerns arise, discuss them. When clarification is needed, facilitate it. The goal is informed decision-making, not binary approve/reject outcomes.

Stay Current on Threat Evolution

Threat actors constantly adapt. The fraud techniques that worked in 2020 have evolved significantly by 2025. AI-generated documents are more sophisticated. Deepfake technology is more accessible. Interview farm operations are more professional. Your screening provider should actively track threat evolution and update detection methodologies accordingly. Static screening procedures become obsolete quickly.



Final Thoughts: The Human Element in a Digital Threat

When I reflect on that first case —the candidate that Anna flagged because “something didn’t feel right”—I’m struck by how much has changed and how much remains the same. The threat has exploded in scale. The technology has become more sophisticated. The regulatory requirements have intensified. But the fundamental dynamic remains unchanged: humans defending against humans.

North Korean operatives, Chinese intelligence officers, organized crime syndicates - they’re humans making strategic decisions about how to infiltrate your organization. They study your hiring processes, identify weaknesses, and craft approaches designed to exploit them. The only effective counter is other humans applying judgment, experience, and intuition to identify threats that purely algorithmic approaches miss.

This is why I call background screening the human firewall. Firewalls in computer networks operate on predefined rules: block this traffic, allow that traffic, inspect everything against known threat signatures. But humans face threats that don’t match existing signatures - novel approaches, sophisticated social engineering, carefully constructed false identities that appear legitimate on the surface.

The human firewall adapts, learns, recognizes patterns, and applies contextual judgment. It’s the critical first line of defense that determines whether a sophisticated threat actor gains trusted access to your organization or gets stopped at the gate. It’s the difference between discovering a North Korean operative during the hiring process versus discovering them two years later when they’re already embedded in your infrastructure, working on multiple projects, and actively exfiltrating data.

Organizations invest millions in cybersecurity -firewalls, intrusion detection, endpoint protection, security operations centers. These are essential investments. But if you’re not investing proportionally in the human firewall—in robust background screening that combines technology with human expertise - you’re leaving your front door unlocked while securing every window. The threat actors know this. The question is: do you?



European Regulatory Response: CER Directive and National Implementation

The European Union has responded to escalating threats against critical infrastructure through comprehensive regulatory frameworks that explicitly address personnel security. The Critical Entities Resilience (CER) Directive (EU) 2022/2557, which member states must implement by October 2024, establishes binding requirements for protecting essential services across energy, transport, banking, financial markets, health, drinking water, wastewater, digital infrastructure, public administration, and space sectors.

CER Directive Key Requirements:

Article 13 of the CER Directive explicitly requires member states to ensure critical entities take “appropriate and proportionate technical, security and organizational measures” to ensure resilience. This includes:

1. Security of premises and infrastructure, including access control measures
2. Personnel security, including verification procedures and background screening
3. Supply chain security, including security-related aspects concerning suppliers and service providers
4. Risk assessment procedures and incident response capabilities
5. Business continuity and crisis management

The directive explicitly recognizes personnel security as a critical pillar of infrastructure resilience. Organizations cannot secure facilities and networks while allowing unvetted individuals—including fraudulent employees and contractors—direct access to sensitive systems. The threat of fake IT workers and infiltrated supply chains directly undermines the CER Directive’s core objectives.

Czech Implementation: Zákon o kritické infrastruktuře (ZKI)

The Czech Republic implemented the CER Directive through Law 266/2025 Sb., the Zákon o kritické infrastruktuře (Critical Infrastructure Act), which entered into force on August 19, 2025. The ZKI establishes comprehensive personnel security requirements that directly address the threat of fraudulent workers infiltrating critical infrastructure operators.

ZKI Personnel Security Requirements:

1. **Scope of Verification:** Organizations must verify the reliability (ověření spolehlivosti) of both internal employees and external contractors with direct or remote access to critical infrastructure premises or systems. This includes IT staff, maintenance

personnel, security personnel, and any third-party service providers who access sensitive systems.

2. **Critical Suppliers:** Not all external contractors require verification—only those from entities essential to ensuring the basic critical infrastructure service. Organizations must properly identify and register these critical suppliers through risk assessment procedures.
3. **Minimum Verification Standards:** At minimum, organizations must verify identity and criminal record (trestní bezúhonnost). For foreign nationals who resided abroad for more than 3 months within the past 3 years, verification must include equivalent foreign criminal record checks. Additional screening depth must be determined based on risk assessment.
4. **Documented Policy Requirement:** Organizations must establish and document a formal reliability verification policy (politika ověřování spolehlivosti) that defines screening procedures, criteria, frequency, and recordkeeping requirements.
5. **Implementation Deadline:** Organizations designated as critical infrastructure must complete verification of existing employees and implement screening for new candidates and suppliers no later than March 1, 2026.
6. **Severe Penalties:** Violations of ZKI requirements carry significant sanctions: fines up to 50 million CZK (approximately €2 million) or 1.5% of annual turnover, whichever is greater. This creates substantial financial liability for organizations that fail to implement adequate personnel security controls.



Alignment with the Threat:

The ZKI requirements directly address the fraudulent IT worker threat documented throughout this white paper. By mandating identity verification and criminal record checks, the law establishes a baseline defense against operatives using fabricated identities. The requirement to verify foreign equivalents for individuals with recent international residence helps detect operatives attempting to exploit gaps in cross-border verification.

The emphasis on supply chain security—requiring verification of critical external suppliers—closes a vulnerability frequently exploited by adversaries. As documented in Case Study 8, infiltrators often target the supply chain as an easier entry point than direct employment. By extending verification requirements to essential third parties, the ZKI reduces this attack surface.

Most importantly, the ZKI creates clear accountability. Organizations can no longer claim that personnel security is someone else's problem. With explicit legal obligations, substantial penalties for non-compliance, and a firm implementation deadline, Czech critical infrastructure operators must now treat employee verification as a core component of security—not an administrative afterthought. This regulatory pressure, combined with the documented threat cases, is finally forcing organizations to recognize that the insider threat begins at the hiring stage.

Detection and Prevention Strategies

Red Flags During Recruitment

Organizations can identify fraudulent candidates by recognizing consistent patterns:

Video Interview Anomalies:

- Camera consistently malfunctioning or disabled despite working microphone
- Video quality issues (frozen frames, lip-sync problems, unnatural facial movements)
- Background noise suggesting call center or shared workspace environments
- Reluctance to adjust camera angle or show surroundings
- Eyes not tracking naturally during conversation (potentially reading from screen)

Response Pattern Anomalies:

- Technical questions answered fluently but personal questions causing hesitation
- Scripted or overly polished responses lacking spontaneity
- Inability to discuss specific details from previous work experience

- Sudden call disconnection when asked unexpected questions about location or identity
- Generic answers about motivations, team collaboration, or workplace culture

Documentation Issues:

- Inconsistencies between LinkedIn profile, resume, and stated experience
- Generic-sounding names (Mike Smith, Thomas Williams) combined with non-Western appearance
- Home addresses located in remote or unpopulated areas
- LinkedIn profiles lacking meaningful engagement or connections
- Request to change mailing address immediately after hire (family emergency excuse)

Payment and Logistics Red Flags:

- Preference for cryptocurrency payment
- Use of payment intermediaries like Ruul.io, Payoneer, or TransferWise
- Frequent changes to banking information
- VoIP phone numbers instead of legitimate mobile carriers

Technical Detection Methods

Organizations should implement technical controls to identify fraudulent workers:

Identity Verification:

- Use document verification services (Regula Forensics, Trustmatic) to detect generated IDs
- Implement biometric verification during onboarding and periodically thereafter
- Mandate in-person verification for roles with system access (drug testing, fingerprinting)
- Verify employment and education history directly with institutions, not through candidate

Network and Device Monitoring:

- Track IP addresses and geolocation of connections to detect VPN/proxy usage
- Monitor for unauthorized remote access software installation
- Flag connections from unexpected geographic regions
- Analyze login patterns for anomalies (odd hours, impossible travel)

Deepfake Detection:

- Request candidates wave hand in front of face during video calls (causes deepfake glitches)
- Ask candidates to turn camera toward window and describe visible surroundings
- Observe for lighting inconsistencies, unnatural facial movements, or audio desynchronization
- Record interviews for forensic analysis if suspicions arise

Behavioral Analysis:

- Ask unexpected personal questions outside scripted technical topics
- Request specific examples of past work with granular details
- Conduct live coding exercises rather than take-home assignments
- Compare interview performance with on-the-job work (different person may be working)



FBI Recommended Practices

The FBI's July 2025 guidance provides specific recommendations:

- Scrutinize identity documents for misspellings and cross-reference information with social media, portfolio sites, and payment platforms
- Verify prior employment and education directly with businesses and institutions, not through candidate-provided contacts
- Require in-person meetings when possible; mandate video with unobscured backgrounds for remote interviews
- Capture interview images for comparison with future meetings to detect person switches
- Analyze payment accounts of all employees, flagging similar documentation or matching banking information
- Send work equipment only to addresses on identification documents; require additional verification for address changes
- Do not grant system access until background checks are complete
- Educate third-party contractors about these threats if using outsourced IT services



Strategic Recommendations

For Individual Organizations

Establish Clear Ownership and Accountability

Assign responsibility for employment fraud prevention to a specific team—ideally a cross-functional group including HR, IT security, legal, and compliance. Create formal policies requiring security review for any role with access to sensitive systems or data.

1. Implement Multi-Layered Identity Verification

Deploy comprehensive background screening that includes document authentication, direct verification of employment and education history, biometric verification, and ongoing monitoring. Consider services like Scout, Trustmatic, or Regula Forensics specializing in fraud detection.

2. Mandate In-Person Verification for Critical Roles

For positions with access to proprietary systems, customer data, or critical infrastructure, require at least one in-person meeting. If impossible due to geographic distance, use trusted local partners for identity verification.

3. Enhance Interview Protocols

Train recruiters and hiring managers to recognize red flags. Mandate video for all remote interviews. Ask unexpected personal questions unrelated to technical skills. Request environmental context (point camera at window, describe neighborhood). Capture and retain interview recordings for forensic analysis if needed.

4. Implement Robust Technical Controls

Monitor network access for unauthorized VPN usage, unusual geographic connections, or suspicious remote access software. Implement device management that prevents unauthorized software installation. Track login patterns and flag anomalies.

5. Scrutinize Contractor and Third-Party Relationships

If using staffing agencies or outsourced development firms, conduct due diligence on their verification processes. Include fraud prevention requirements in contracts. Periodically audit contractor identity verification.

6. Establish Post-Hire Monitoring

Conduct security onboarding review within first weeks of employment. Periodically re-verify identity. Monitor for signs of multiple concurrent employment (inconsistent availability, poor work quality, unusual working hours). Track data access patterns for anomalies.

For the Background Screening Industry

Develop Specialized Fraud Detection Services

Background screening firms should offer comprehensive packages addressing this threat: AI-powered document authentication, deepfake detection during video verification, direct employment and education verification (not candidate-provided contacts), geographic verification and IP analysis, and continuous monitoring services.

Educate Clients

Proactively warn clients about this threat. Provide training materials for HR teams and hiring managers. Share case studies and red flag indicators. Position screening services as security investments, not administrative overhead.

For European Policymakers

Create European Digital Work Identity Standard

Develop a unified EU Work ID system leveraging eIDAS 2.0 infrastructure. Enable workers to verify identity once with government authorities, then use cryptographic credentials for employment verification. This would dramatically reduce verification burden while improving security.

Mandate Identity Verification for Critical Infrastructure

Under NIS2 and Cyber Resilience Act frameworks, require organizations in critical sectors to implement verified identity systems for all personnel with system access. Establish clear liability for failures to verify employee identity that result in breaches.

Establish European Threat Intelligence Sharing

Create EU-wide database of confirmed fraud attempts, similar to financial industry blacklists. Enable employers to check whether candidates or staffing agencies have history of fraud. Coordinate with ENISA to provide centralized threat intelligence and guidance.

Reduce Bureaucratic Barriers

Streamline legitimate hiring processes to reduce pressure for shortcuts. Digitize verification workflows. Harmonize cross-border employment regulations. When legal compliance is simpler, organizations can invest more resources in security.

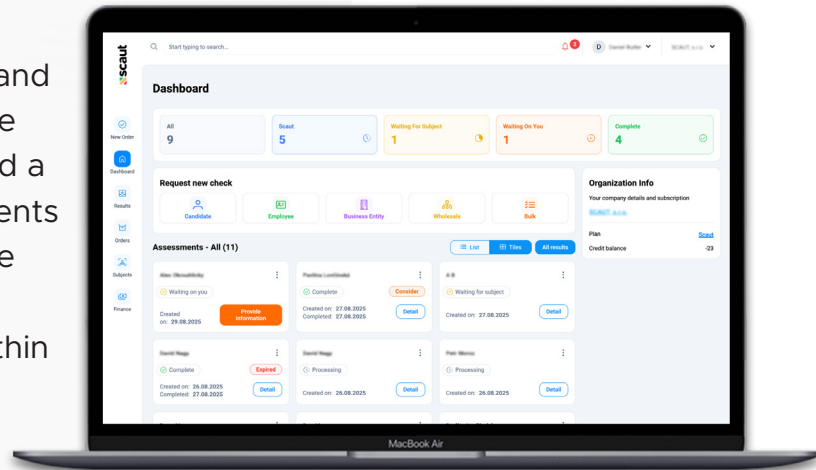


Scaut: Your Partner in Secure Hiring

As Central Europe's leading screening and workforce monitoring platform, Scaut offers GDPR-compliant tools to verify candidates and monitor workforces. Our platform integrates automation with analyst expertise for precision verification, specifically designed to detect and prevent the sophisticated infiltration threats documented throughout this white paper.

The Solution

Scaut is an online platform for employee and extended workforce screening. We enable companies and their supply chains to build a trusted workforce and fulfill the requirements of cyber security and critical infrastructure legislations including NIS2, CER Directive, Czech ZKI, and ISO 27001. Deployable within hours, not weeks—you can trust Scaut.



Our solutions deliver:

1. **Cost saving and security:** We take care of both the complexity and the compliance. Do all your workforce screening in one place with no loose data ends. Enjoy GDPR compliance and ISO 27001 certified processes.
2. **A verified workforce:** Pre-employment screening, workforce monitoring, KYC checks, security clearance, or identity verification—we can verify it all. Our tools specifically detect AI-generated documents, fake identities, and interview farm patterns.
3. **Audit with confidence:** Stay compliant and prove you're doing what it takes to protect your industry. Our internal use reports and oversight access roles keep you audit-ready for ZKI, NIS2, CER, and other regulatory requirements.
4. **A complete solution:** The Scaut platform combines the power of SaaS connectivity and automation with the expertise of our human analysts. We have everything covered from document forensics to behavioral analysis.

The Platform

1. **Modern interface:** Intuitive design simplifies process management for HR teams and security officers.
2. **Automated checks:** Our verification processes save time and provide real-time information where available, including instant sanctions list screening and identity document validation.

3. **HRIS and ATS integration:** Seamless connectivity via open API for streamlined recruitment and data management.
4. **Continuous monitoring:** Ensures ongoing security for employees, partners, and suppliers—critical for detecting post-hire threats.
5. **Scalable system:** Suits companies of all sizes, from startups to enterprises, with options from pay-per-check to comprehensive subscription plans.
6. **Cutting-edge technologies:** Continuously integrating forensic and analytical tools including deepfake detection, IP geolocation analysis, and document authenticity verification to deliver top-tier screenings with unmatched accuracy.

Supply Chain Security

Can you risk knowing nothing about the people in your supply chains? Is there strange activity going on with your remote IT workers? What do you know about the people employed by the third parties you work with? Not only is it best practice to ensure your staff are safely vetted, but also your contractors, business partners, and all the companies that make up your supply chains.

Are you protected from these risks?

1. **Security Threats:** Without proper background checks, employees with criminal records or affiliations with malicious entities might infiltrate the supply chain, leading to theft, sabotage, and unauthorized access to sensitive information.
2. **Operational Disruptions:** In critical operations involving perishable goods or just-in-time manufacturing, even minor disruptions can cascade through the entire supply chain.
3. **Regulatory Violations:** Employing individuals without proper work authorization or those with regulatory breach histories can expose companies to significant legal risks, particularly under ZKI and CER Directive requirements.
4. **Insider Threats:** Employees with malicious intent can exploit access credentials to leak confidential data, manipulate processes for personal gain, or collaborate with competitors—or hostile state actors.
5. **Reputational Damage:** Whether it's a data breach, product recall, or regulatory fine, the fallout from employing unvetted personnel can be long-lasting and detrimental to the company's public image.

Organizations investing in people controls like screening have been shown to experience decreased losses and faster fraud detection. You should insist on a comprehensive screening process for all personnel in your supply chain, including background checks and continuous monitoring. Talk to Scout today.

Contact Scaut

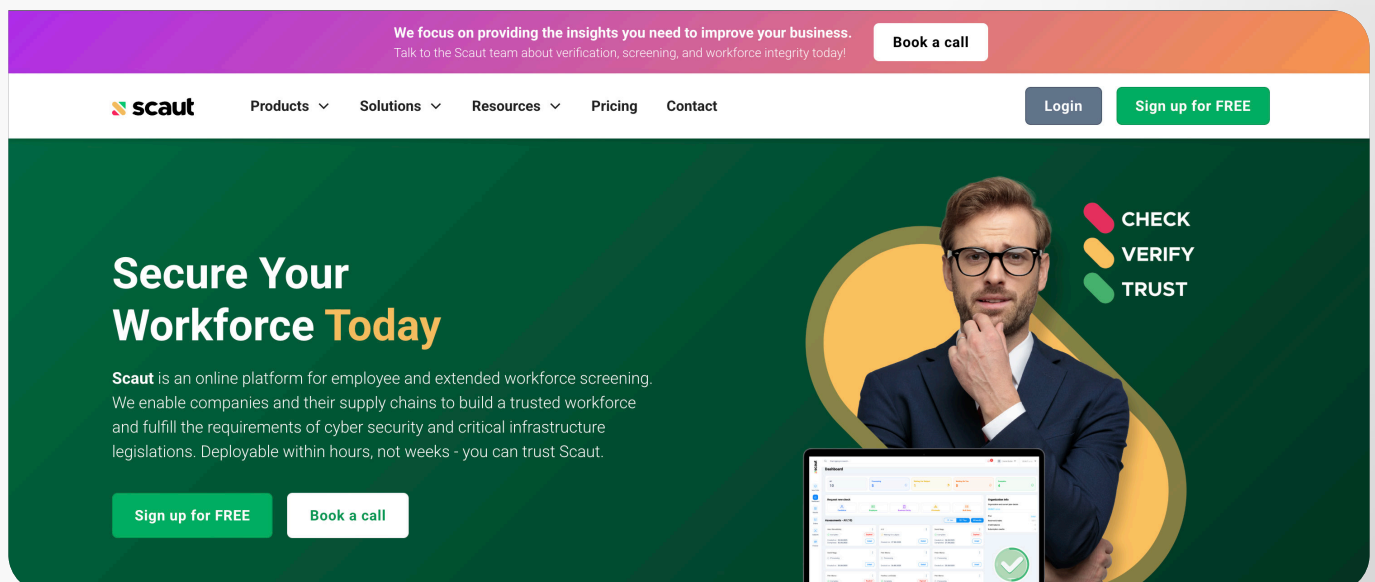
We manage your recruitment risks globally. Our focus is on helping organizations of all sizes hire trusted candidates or contractors while meeting compliance regulations, all in a streamlined and scalable platform.

With Scaut you get:

1. Rapid screening results at scale
2. State-of-the-art technologies including AI detection
3. Compliance with NIS2, CER, SOC2, Czech ZKI, and ISO 27001
4. Secure workforce supply chain verification
5. Quantifiable hiring due diligence
6. One-stop verification of key metrics
7. Tailored screening solutions
8. Improved team quality and efficiency
9. No unnecessary paperwork
10. Global screening coverage
11. Instant verifications where available

Background checks are crucial to your organization's success. Hire good people, reduce losses, and increase productivity.

Visit <https://www.scaut.com> or contact our team today to discuss your organization's screening needs.



The screenshot shows the Scaut website homepage. At the top, a purple and orange gradient banner contains the text "We focus on providing the insights you need to improve your business. Talk to the Scaut team about verification, screening, and workforce integrity today!" and a "Book a call" button. Below this is a white navigation bar with the Scaut logo, links for "Products", "Solutions", "Resources", "Pricing", and "Contact", and buttons for "Login" and "Sign up for FREE". The main content area has a dark green background. On the left, the headline "Secure Your Workforce Today" is displayed, with "Today" in orange. Below it, a paragraph describes Scaut as an online platform for employee and extended workforce screening. At the bottom left of this section are "Sign up for FREE" and "Book a call" buttons. On the right, a man in a suit and glasses is shown in a circular frame, with a laptop displaying the Scaut interface in front of him. To his right, three colored circles (red, yellow, green) are stacked vertically with the labels "CHECK", "VERIFY", and "TRUST" respectively.

Sources and Citations

This white paper synthesizes information from authoritative sources including government agencies, cybersecurity firms, research organizations, and direct operational experience. All statistics, case studies, and threat intelligence are derived from the following documented sources:

Government and Law Enforcement Sources

1. **U.S. Department of Justice:** “Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote IT Worker Fraud.” Available at: <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>
2. **DOJ - Chapman Case:** “Arizona Woman Sentenced for \$17M Information Technology Worker Fraud Scheme.” Available at: <https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue>
3. **DOJ US Attorney’s Office:** “Arizona Woman Sentenced in \$17M IT Worker Fraud Scheme That Illegally Generated Revenue for North Korea.” Available at: <https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north>

Cybersecurity Firms and Threat Intelligence

1. **Microsoft Security:** “Jasper Sleet: North Korean remote IT workers’ evolving tactics to infiltrate organizations.” Microsoft Security Blog. Available at: <https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/>
2. **CrowdStrike (Fortune):** “North Korean operatives have infiltrated hundreds of Fortune 500 companies.” Available at: <https://cyberscoop.com/north-korea-workers-infiltrate-fortune-500/>
3. **Okta Threat Intelligence:** “North Korea’s IT Workers expand beyond US big tech.” Okta Newsroom. Available at: <https://www.okta.com/newsroom/articles/north-korea-s-it-workers-expand-beyond-us-big-tech/>
4. **DTEX Systems:** “Exposing DPRK: Nation-State Threat Actors.” Available at: <https://www.dtexsystems.com/exposing-dprk/>
5. **Palo Alto Networks Unit 42:** “Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation.” Available at: <https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/>

Industry Research and Analysis

1. **Gartner Research:** “Gartner Survey Shows Just 26% of Job Applicants Trust AI Will Fairly Evaluate Them.” Press release, July 31, 2025. Available at: <https://www.gartner.com/en/newsroom/press-releases/2025-07-31-gartner-survey-shows-just-26-percent-of-job-applicants-trust-ai-will-fairly-evaluate-them>
2. **HR Dive:** “By 2028, 1 in 4 candidate profiles will be fake, Gartner predicts.” Available at: <https://www.hrdive.com/news/fake-job-candidates-ai/757126/>
3. **Fortune:** “North Korean IT worker infiltrations exploded 220% over the past 12 months.” August 4, 2025. Available at: <https://fortune.com/2025/08/04/north-korean-it-worker-infiltrations-exploded/>
4. **Crowell & Moring:** “From Deepfakes to Sanctions Violations: The Rise of North Korean Remote IT Worker Schemes.” Available at: <https://www.crowell.com/en/insights/client-alerts/from-deepfakes-to-sanctions-violations-the-rise-of-north-korean-remote-it-worker-schemes>
5. **Fordham University:** “America’s Best Remote Workers Might Be North Korean.” Fordham Now. Available at: <https://now.fordham.edu/university-news/americas-best-remote-workers-might-be-north-korean/>
6. **Becker’s Hospital Review:** “North Korean IT workers targeting healthcare jobs—85 interviews detected in 2025.” Available at: <https://www.beckershospitalreview.com/healthcare-information-technology/north-korean-it-workers-targeting-healthcare-jobs-report/>

News and Investigative Journalism

1. **CNN Interactive:** “How North Korean IT workers leverage AI and vulnerable Americans to infiltrate US companies.” August 5, 2025. Available at: <https://www.cnn.com/interactive/2025/08/05/world/north-korea-it-worker-scheme-vis-intl-hnk/index.html>
2. **Wired:** “Leak Reveals the Workaday Lives of North Korean IT Scammers.” Available at: <https://www.wired.com/story/leaked-data-reveals-the-workaday-lives-of-north-korean-it-scammers/>
3. **CyberScoop - Okta Report:** “North Korea IT worker scheme swells beyond US companies.” Available at: <https://cyberscoop.com/north-korea-it-worker-global-scheme-okta/>
4. **The Record:** “North Korea IT worker scheme expanding to more industries beyond tech.” Available at: <https://therecord.media/north-korea-it-worker-scheme-expands-outside-us-tech>

Note on Methodology: This white paper integrates information from multiple authoritative sources to provide a comprehensive threat assessment. Where specific statistics or claims are referenced in the text, they are drawn from the sources listed above. All case studies are based on publicly documented incidents or direct operational experience from Scout.com background screening operations. URLs were verified as accessible as of October 2025.

Additional Resources: For the most current threat intelligence and updates on North Korean IT worker infiltration campaigns, organizations should monitor advisories from the FBI Internet Crime Complaint Center (IC3), CISA cybersecurity alerts, and ENISA threat landscape reports. Scout.com maintains an updated blog with European-focused threat intelligence at scout.com/blog.



Conclusion: The Urgency of Action

The invisible workforce is already here. Sophisticated state-sponsored operatives have successfully infiltrated thousands of organizations globally, generating hundreds of millions of dollars in illicit revenue while simultaneously stealing intellectual property, installing malware, and positioning themselves for future cyberattacks.

This is not a theoretical threat or a distant concern. It is happening now, at scale, with alarming success rates. The technology enabling these operations—deepfakes, AI-powered identity construction, encrypted communications—advances faster than defensive measures. What took specialized expertise and expensive equipment two years ago can now be accomplished in an hour with consumer-grade tools.

The most concerning aspect is the exploitation of trust. Organizations have built entire remote work cultures on the assumption that people are who they claim to be. Video calls, digital documents, and online interviews replace in-person verification. This efficiency has created exploitable vulnerabilities.

Europe faces particular risk. The fragmented regulatory environment, bureaucratic complexity, and lack of centralized threat awareness create opportunities for adversaries. While the United States benefits from unified FBI warnings and coordinated law enforcement, European organizations often lack even basic awareness of the threat.

The solution requires action at multiple levels:

The cost of inaction far exceeds the investment in prevention. A single successful infiltration can result in millions in stolen intellectual property, regulatory fines, and reputational damage. The ChapmanCost data breach averages \$4.88 million. A major IP theft or ransomware incident can be catastrophic.

Most importantly, this threat connects directly to national security. The revenue generated funds weapons development, sanctions evasion, and destabilization campaigns. Every fraudulent hire provides operational intelligence about Western corporate infrastructure. Some operatives are actively deploying on Russian frontlines in Ukraine—trained cyber warriors who previously infiltrated Fortune 500 companies.

The invisible workforce is a clear and present danger.

Recognition of the threat is the first step. Action must follow immediately.

Key Statistics Summary

The following table summarizes critical statistics documenting the scale and impact of this threat:

Metric	Value
Growth in infiltrations (12 months)	220% increase
Chapman laptop farm revenue	\$17.1 million
Fraudulent hires (Chapman operation)	309 positions / organizations
Job interviews tracked (Okta, 2021-2025)	6,500+ across 5,000+ companies
Healthcare interviews detected (2025)	85 organizations
Non-U.S. company targets	27% of interviews
Time to create deepfake (no experience)	70 minutes
Average data breach cost (global)	\$4.88 million
Average healthcare breach cost	\$11 million
Cyber incidents in Europe (EU, 2024)	2x increase vs. 2023
Annual cyber damage in EU	€180 billion

Sources: FBI IC3, CrowdStrike, Okta, Unit 42 (Palo Alto Networks), IBM Cost of Data Breach Report, ENISA, European Commission

About This Report

This white paper was developed to raise awareness of a critical and rapidly evolving cybersecurity threat facing organizations worldwide. The research synthesizes information from multiple authoritative sources including:

- Federal Bureau of Investigation (FBI) public service announcements and Internet Crime Complaint Center advisories
- Google Threat Intelligence Group (Mandiant) analysis and reporting
- Unit 42 threat research from Palo Alto Networks
- CrowdStrike Counter Adversary Operations investigations
- Okta Threat Intelligence assessments
- DTEX Systems Insider Intelligence and Investigations analysis
- European Union Agency for Cybersecurity (ENISA) reporting
- Direct case studies from Czech cybersecurity professionals and background screening firms
- Court documents and law enforcement actions including the Chapman laptop farm prosecution

This document is intended for use by:

- Chief Information Security Officers (CISOs) and security leadership
- Human Resources directors and talent acquisition teams
- Executive leadership and board members responsible for enterprise risk
- Background screening professionals and identity verification providers
- Legal and compliance officers addressing regulatory requirements
- Government and policy professionals developing cyber defense strategies

For questions, additional information, or to discuss how background screening services can address these threats, please contact your security and compliance teams or consult with specialized verification providers

This document may be shared and distributed freely to raise awareness of this critical threat. Attribution to Scaut is appreciated, but not required.

The risks

Can you risk hiring people you **know nothing** about?

There are many reasons for you to ensure compliance and security in your hiring process. Are you doing enough to mitigate the risks your business is facing?

Are you protected from these risks?

Non-compliance

With EU and national regulatory requirements to secure critical infrastructure (NIS 2, CER and more), obligations to have a secure workforce are increasing.

Supply chain vulnerability

With the ever increasing ability to work remotely, contractors with hostile intent can easily assume false identities and join your team. The supply chain is often used as a vector of attack in cyber-crime.

Identity theft

Fraudulent employees can misuse colleagues' or clients' personal information for their own enrichment or other illegal activities.

Data theft

Unauthorized access to company data can lead to its theft, which puts client privacy and company trade secrets at risk.

Financial fraud

From payment diversion to asset misappropriation, financial fraud can cause huge financial losses for companies.

Reputational damage

Hiring the wrong person can cause significant loss to financial capital, social capital and/or market share.



Recruitment fraud accounts for **24 Billion GBP** lost in the UK alone

The Association of Certified Fraud Examiners estimates **organizations lose an estimated 5% of their annual revenue to fraud**, with a significant portion attributed to **actions taken by insiders.**

Organizations investing in people controls like screening have been shown to experience smaller losses and detect fraud more quickly. **Talk to Scout today.**

Alert: Fake Software Engineers from China Infiltrating European Businesses

Companies in Europe have recently encountered a remarkable phenomenon: IT candidates who, according to the documents they provided to their prospective employer, should be sitting at a computer somewhere in Europe are actually in China.

This was the case of one of the Czech technology startups that MF DNES met (due to the sensitivity of the case, the editors did not mention the name of the company).

A person interested in the job of a full-stack lead developer applied for the job via the social network LinkedIn. According to the documents he provided to the company, he was a Danish citizen living in Denmark. He successfully passed several rounds of the recruitment process, which also tested his programming skills. However, the information he provided to his prospective employer did pass the rigorous screening process at Scaut.

"When we followed the trail of the linkedin profile, we found that it was connected with other suspicious profiles. They all have common characteristics, they try to give the impression that these people are graduates of European universities and usually work remotely for a long time, for example from Serbia or Estonia," says Petr Moroz, CEO of Scaut, which screened job candidates for the company.

The network of hundreds of LinkedIn profiles then converges on the Chinese city of Dandong, a city of two million near the border between China and North Korea. The city is home to, among other things, a Chinese army base.

That the Chinese intelligence services may be behind the activities of the 'fake A.I.' is just one theory. However, the largest domestic secret service, the BIS counterintelligence agency, has long warned against Chinese activities on Czech territory, and so has the FBI in its public warnings from...

**Learn more about protecting your company.
Talk to Scaut today.**

source: excerpt from scout.com/en/blog



Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.



Because integrity matters.