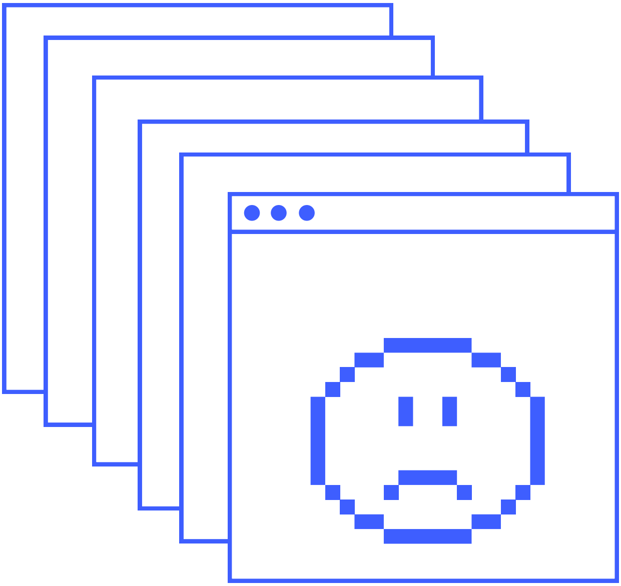
Deepfake Fraud Prevention

Practical Strategies to Detect Fake IT Workers



VIDOC
Security lab

Authors

- **Klaudia Kloc** in
  Chief Executive Officer at Vidoc Security Lab
- **Dawid Moczadło** in
  Chief Technology Officer at Vidoc Security Lab
- **Zuzanna Mówińska** in
  UX/UI & Creative Designer at Vidoc Security Lab
- **Paulina Michalczyk** in
  Head of Operations at Vidoc Security Lab
- **Monika Kamińska** in
  Attorney & Founder at Truesty
- **Piotr Brzyski** in
  AI Consultant & Founder of Zetatech

Reviewers

- **Aarti Samani** in
  Chief Executive Officer at Shreem Growth Partners

Presentation

In addition to this ebook, we have prepared a **dedicated presentation** on detecting fake candidates. It includes numerous visual elements that are not featured here, making it perfect for sharing with your team. If you're interested, feel free to reach out to us via email **contact@vidocsecurity.com** to get access.

Table of Contents

Table of Contents

Introduction

At Vidoc Security Lab, we came across a job applicant who seemed perfect on paper. But something felt off. We quickly realized they were using AI tools to fake their answers, and even deepfake software to change their appearance during video calls. **It made us realize how easy it would be for someone without a security background to miss the signs.**

This playbook is based on our experience and stories from other startup founders and hiring managers who've faced similar issues. We also spoke with many experts to give you practical advice that's based on real-world cases and examples.

Who is it for? HR professionals, recruiters, hiring managers, cybersecurity teams, and anyone involved in recruitment and applicant screening processes.

After Reading This Guide, You Will Be Able To:

⇛ Reliably spot telltale signs of AI-assisted fraud during video interviews,

⇛ Implement a verification system that catches 90% of fake candidates before they reach technical interviews,

⇛ Ask the right questions that genuine candidates can answer but AI imposters cannot,

⇛ Protect your company from harmful actors seeking to access sensitive information,

⇛ Verify candidate identities using both low-tech and technology-assisted methods,

⇛ Create an interview process that makes it difficult for deepfakes to succeed,

⇛ Know exactly what to do when you suspect you're interviewing a fake candidate,

⇛ Train your HR team to recognize and respond to increasingly sophisticated AI deception.

Figure 1. Online interviews are very common

New Challenges in Online Interviews

Every day, thousands of job interviews take place around the world. According to a study by Indeed from 2021, **82% of companies switched to online hiring**, and many have continued using this method *(Lewis L. (2021, October 14) 2021 Hiring Trends Report. Indeed For Employers. [https://www.indeed.com/lead/2021-hiring-trends-report?hl=en&co=US])*. Online interviews have opened up new opportunities — experienced candidates from around the world can now join teams in companies abroad. The golden era of online interviews started to fade with the launch of ChatGPT at the end of 2022 *(Open AI (2022, November 30) Introducing ChatGPT. [https://openai.com/index/chatgpt/])*. **This new technology has boosted the growth of all industries but also created security gaps and opportunities for abuse.** It has especially impacted the HR and cybersecurity industries.

Backstory

The COVID-19 pandemic changed many industries. With limited in-person contact, many switched to online work. HR was one of the industries that quickly adapted to this new way of working. **Recruitment interview fraud started appearing early on**, but it reached its peak after the launch of the revolutionary AI technology — ChatGPT.

Artificial Intelligence, a technology that learns to perform tasks, recognize patterns, process natural language, and make decisions like a human, quickly took over the HR world *(Wikipedia (2025, June 8) Artificial intelligence. [https://en.wikipedia.org/wiki/Artificial_intelligence])*. Candidates noticed better results in getting job interviews after polishing their applications with ChatGPT. They could also edit cover letters faster and more easily, tailoring them to specific companies and job postings.

The surge in job applications, particularly for remote roles, reached unprecedented levels. This created a new challenge — with so many well-crafted applications, standing out became incredibly difficult. As a result, some candidates resorted to exaggerating their experience and skills on their CVs to gain an edge.

> **[...] One Reddit user built an AI agent that "automatically applied for 1,000 jobs and got 50 interviews"—the post went viral, and their GitHub project racked up ~27,000 stars, signaling just how widespread this shift has become. ~ Kamil Ruczynski from AI+consumer**

Figure 2. AI+consumer (2025, February 12). AI x Hiring. [https://aiconsumer.substack.com/p/ai-x-hiring]

5.24B

Approx. ChatGPT.com visits per month

(Semrush Traffic Stats, May 2025)

79%

Recruiters believe AI will soon be able to make hiring decisions

(Tidio, 2025)

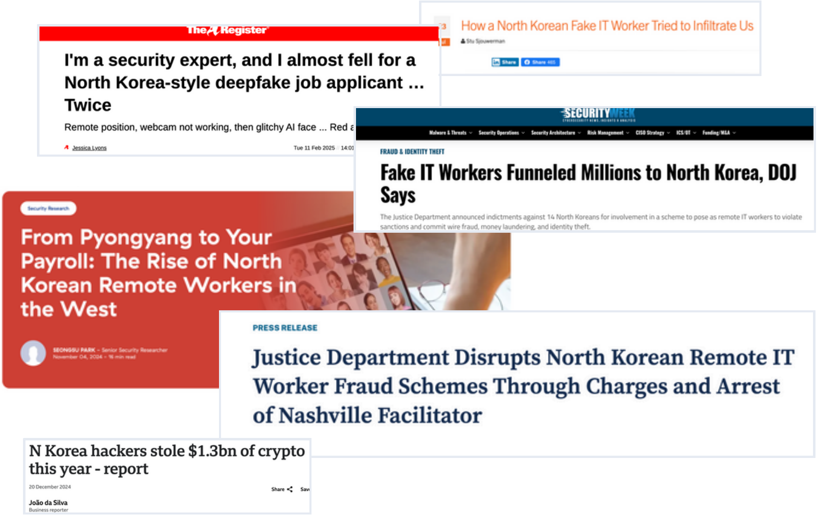
$4.88M

The average cost of data breach

(IBM, 2024)

Originally, AI was used to match applications with job descriptions, helping recruiters find the right candidates more efficiently. However, as AI tools evolved, so did their misuse.

Global Threats



The Register

I'm a security expert, and I almost fell for a North Korea-style deepfake job applicant … Twice

Remote position, webcam not working, then glitchy AI face ... Red a

Jessica Lyons Tue 11 Feb 2025 // 14:01

How a North Korean Fake IT Worker Tried to Infiltrate Us

Stu Sjouwerman

Share Share 465

SECURITYWEEK

Malware & Threats · Security Operations · Security Architecture · Risk Management · CISO Strategy · ICS/OT · Funding/M&A

FRAUD & IDENTITY THEFT

Fake IT Workers Funneled Millions to North Korea, DOJ Says

The Justice Department announced indictments against 14 North Koreans for involvement in a scheme to pose as remote IT workers to violate sanctions and commit wire fraud, money laundering, and identity theft.

Security Research

From Pyongyang to Your Payroll: The Rise of North Korean Remote Workers in the West

SEONGSU PARK – Senior Security Researcher
November 04, 2024 – 16 min read

PRESS RELEASE

Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator

N Korea hackers stole $1.3bn of crypto this year - report

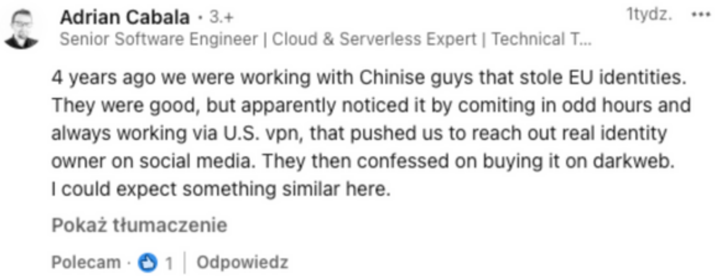
20 December 2024

Share Sav

João da Silva
Business reporter

The rise of fake remote workers using AI [1]

Governments around the world have recognized the ethical risks of AI. Its use in job interviews has made corporate espionage easier, allowing fake candidates to manipulate the hiring process, gain access to sensitive company information, and even demand ransom.



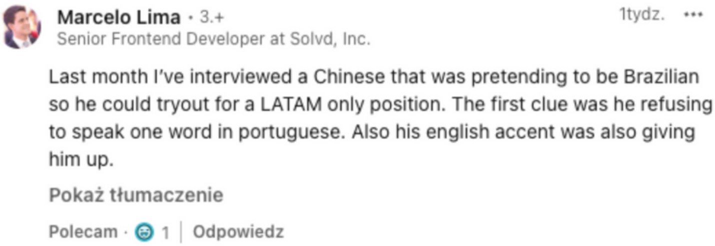
Adrian Cabala · 3.+ 1tydz.
Senior Software Engineer | Cloud & Serverless Expert | Technical T...

4 years ago we were working with Chinise guys that stole EU identities. They were good, but apparently noticed it by comiting in odd hours and always working via U.S. vpn, that pushed us to reach out real identity owner on social media. They then confessed on buying it on darkweb.
I could expect something similar here.

Figure 3. Comment by Adrian Cabala
under a LinkedIn post by Dawid Moczadło (2025)

In 2024, the U.S. Justice Department took down a North Korean fraud scheme involving remote IT jobs *(Archive of U.S. Department of Justice (2024, August 8) Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator, [https://www.justice.gov/archives/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and])*.

Matthew Isaac Knoot used a stolen identity to pose as a U.S. citizen. **He installed unauthorized software on company laptops, allowing North Korean hackers to gain access and commit fraud.** He was also part of a money laundering scheme, funneling earnings from remote IT jobs to accounts connected to North Korea and China.



Marcelo Lima · 3.+
Senior Frontend Developer at Solvd, Inc.
1tydz.

Last month I've interviewed a Chinese that was pretending to be Brazilian so he could tryout for a LATAM only position. The first clue was he refusing to speak one word in portuguese. Also his english accent was also giving him up.

Figure 4. Comment by Marcelo Lima under a LinkedIn post by Dawid Moczadło (2025)

The Rise of AI in Recruitment Fraud

With more hiring moving online, some job seekers are using AI to cheat—not just for answers, but to fake entire interviews. Deepfake videos and AI-generated voices can make an unqualified candidate appear highly skilled, making it difficult for hiring managers to verify who they are actually speaking to.

The risk is real. Companies may end up hiring people who lack the necessary skills, leading to errors, delays, and security threats. In fields like software development and cybersecurity, an unqualified hire could overlook critical vulnerabilities, increasing the risk of hacks and data breaches.

Figure 5. Online interviews are very common

Recruitment Process - Strange Incidents + Tips

At Vidoc Security Lab, we started the recruitment and hiring process back in 2024 to find an experienced developer. Our ideal candidate was someone with a background in both startups and large companies. The moment we posted the job ad on LinkedIn, applications flooded in so quickly that **it became evident some were submitted automatically using bots** (some people admitted to using it later in the process).

TIP #1
If you get a bunch of applications right after posting a job,
it's probably automation.

> **"It's not possible that 3 people already applied in the first second. Later, some devs admitted that they have automation that automatically submits their applications to new ads." ~ Paulina Michalczyk, Head of Vidoc Security Lab**

Figure 6. Quote About Automated Job Applications From Paulina Michalczyk (2025)

Paulina, filtered through the applications, selecting only those that met our criteria. However, during the initial interviews, an unsettling pattern emerged.

Candidates with Eastern European-sounding names often turned out to have thick non Eastern-European accents (often Asian), and some struggled with basic English communication. Many of them refused to turn on their cameras, citing technical issues.

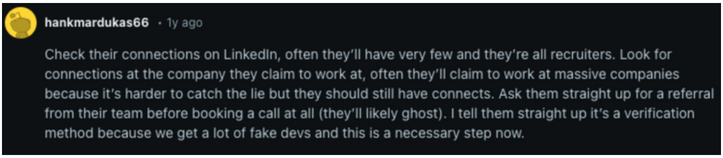
TIP #2
In remote video interviews,
cameras should always be on.
Refusal is a red flag.

> **"Once, we received an application from someone with a Polish name. In Polish applications, it's common to include an address — but this person listed the District Court in Warsaw as their address." ~ Paulina Michalczyk, Head of Vidoc Security Lab**

Figure 7. Quote About Fake Address in Job Application From Paulina Michalczyk (2025)

Many of these applicants didn't even answer simple questions like 'What is your hobby?' Instead, they just read responses straight from some AI chat.

TIP #3
Always double-check details like
address and phone number-
-they're often fake.



hankmardukas66 · 1y ago

Check their connections on LinkedIn, often they'll have very few and they're all recruiters. Look for connections at the company they claim to work at, often they'll claim to work at massive companies because it's harder to catch the lie but they should still have connects. Ask them straight up for a referral from their team before booking a call at all (they'll likely ghost). I tell them straight up it's a verification method because we get a lot of fake devs and this is a necessary step now.

Figure 8. Comment by hankmardukas66 under a Reddit post "Inundated with fake candidates" (2024)

TIP #4
Check their LinkedIn connections--fake profiles often have weak networks.

Then, we conducted open-source intelligence on them, checking their online presence. **Open-source intelligence** is the collection of data gathered from open sources like Social Media (*Wikipedia (2025, June 13) Open-source intelligence [https://en.wikipedia.org/wiki/Open-source_intelligence]*), *online: February 20, 2025*). **Aside from a LinkedIn profile, there was nothing.**

TIP #5
Newly created, or inactive LinkedIn profiles with AI-enhanced photos might be fake.

The LinkedIn profiles seemed suspicious — many had no profile pictures, and those that did looked artificially generated, though difficult to verify. Most profiles were inactive, with only a handful of outdated posts. Over time, a pattern emerged: **identical CVs were being submitted under different Eastern European names, each linked to a freshly created LinkedIn profile with AI-"enhanced" photos.**

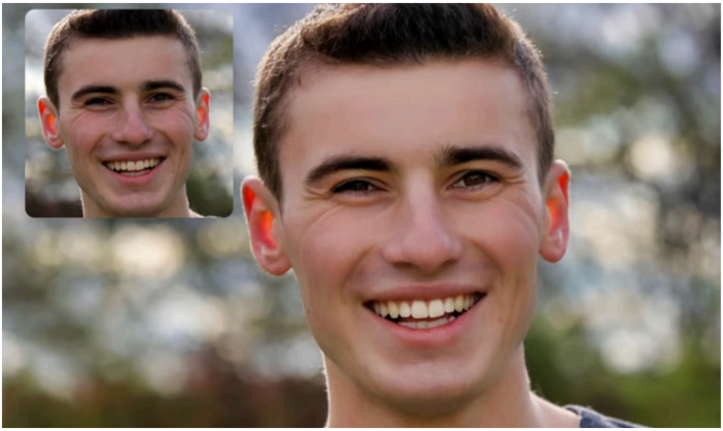


Figure 9. AI Image Enhancement by BeFunky, Retrieved on February 27, 2025

Their experience and education didn't add up either. As mentioned before, they had Eastern-European (often Polish) names, but their backgrounds often included impressive roles at companies like Meta — usually only abroad. All of these were clear red flags in hindsight. However, **for those unfamiliar with AI and deepfake-assisted job fraud, spotting the deception in real time can be challenging.** Surprisingly, these candidates performed well enough during the initial screening to advance to the next stage — a technical interview with Vidoc Security Lab's Chief Technology Officer, Dawid Moczadło.

TIP #6
Almost "perfect" candidate with experience in top-tier companies like Meta, Google - to check.

TIP #7
North American education and multinational roles, yet poor English skills - proceed with caution.

The Deepfake Interview

A candidate, Bratislav, reached out to Klaudia Kloc, CEO of Vidoc Security Lab, via LinkedIn, asking if we were hiring. **He had a Slavic name, claimed to live in Serbia, and had a strong tech background with experience at decent companies.** He followed up several times. As soon as we needed to hire a developer, we contacted him.

During his initial interview, **he refused to turn on his camera**, claiming it was broken. When he reached the technical interview stage with our CTO, Dawid Moczadło, he repeated the excuse. However, for security reasons, the interview couldn't proceed without video, so it was rescheduled.

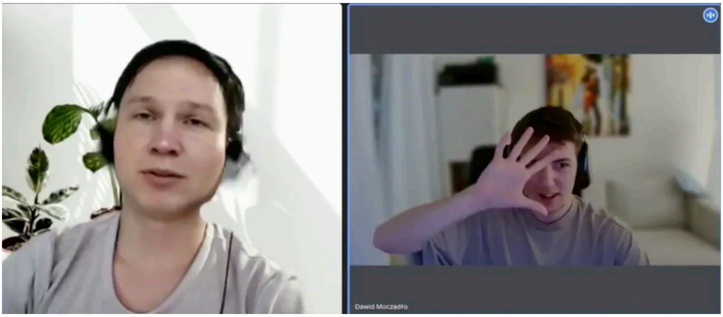


Figure 10. Screenshot From the Interview With Bratislav and Dawid (2025)

By the evening, Bratislav had fixed his camera, but something felt off. Dawid asked him a few questions and quickly grew suspicious that he was using a deepfake. AI-generated deepfakes aren't flawless yet, and Dawid knew how to test them.

Dawid noticed that Bratislav's **face didn't quite match his neck.** He had a **strong foreign accent**, which didn't match his country of origin. **His answers felt like they were straight from ChatGPT** — structured like bullet points, overly polished, and lacking any natural flow.

TIP #8

A strong foreign accent that doesn't match their stated nationality can be a red flag, but be mindful of bias.

There are tools now that can alter eye movement on camera, making it appear as if someone is looking straight ahead, even when they're actually reading from a script. This made it even harder to detect deception at first.

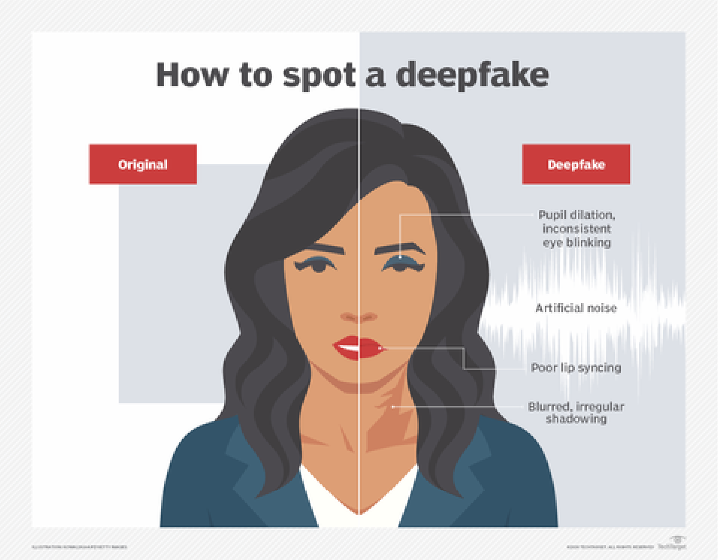


Figure 11. How to detect deepfakes manually and using AI by Tech Target, Retrieved on February 27, 2025

Dawid had one final test. When he was almost certain that Bratislav was lying about his identity, **he asked him to place his hand in front of his face.** AI deepfake technology, while advanced, isn't perfect yet (which is a concerning sign for the future). Covering part of the face often causes the deepfake to break. At first, Bratislav hesitated, asking if this was a joke, and outright refused. Then, after some insistence, he reluctantly raised his hand — but carelessly, in a way that didn't actually cover his face. That was enough confirmation. Dawid immediately ended the call.

TIP #9

Ask them to cover a part of their face - AI will probably break.

Figure 12. A simple face cover test can reveal use of deepfake technology in an online interview

Other Ways to Deal with AI Actors

Our final stage of the interview process always takes place on-site, where we spend the entire day with the candidate. While it can be challenging to bring in applicants from outside Poland or the USA on a startup budget, it's essential for us to truly get to know them. We anticipate that **on-site interviews may become more popular again** in the future.

TIP #10

At least the final stage of the hiring process should always be on-site.

To detect potential impersonation, we conduct thorough open-source intelligence checks. Because most people maintain some presence on widely used social media platforms, **a complete absence of such activity can be a red flag.** Analyze the photos. Sometimes if you feel something is off with the photo, but you can't point out what - check the fingers, since AI cannot create them right.

TIP #11

Conduct open source intelligence.

We also request references from previous employers. This not only helps us verify a candidate's background but also confirms the authenticity of the information provided. Unfortunately, some individuals try to hold multiple jobs at once to increase their income

TIP #12

Contact previous employers.

We also request references from previous employers. This not only helps us verify a candidate's background but also confirms the authenticity of the information provided. Unfortunately, some individuals try to hold multiple jobs at once to increase their income or gain access to proprietary code, which they may then misuse.

TIP #12
Contact previous employers.

It's crucial to share knowledge about these risks. AI can be dangerous if misused, and many people — especially those not closely following AI developments — find it difficult to spot a fabricated face on a video call.

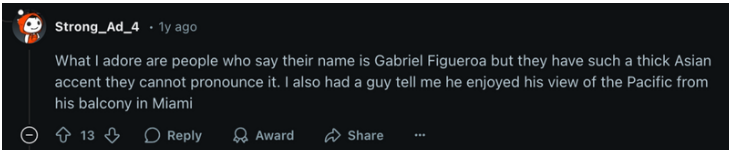
Telltale signs include lips that barely move, eyes that appear abnormal, or a mismatch between the face and the neck. Currently, AI tools often leave a visible line where the generated face meets the neck. Moreover, some have noted that virtual backgrounds can appear unnatural, leading to skepticism. Hiring managers frequently prefer a simple blur effect or no background alteration at all.

TIP #13
Pay attention to details. Does their mouth movement seem natural?

From a legal perspective, **impersonating others or providing false information in applications can result in significant penalties in various jurisdictions worldwide.** For instance, in the United States, federal statutes address identity theft and fraud with serious consequences, while Polish law similarly enforces strict measures against impersonation and dishonest representation.

If you suspect a candidate might be fake during an interview, try asking specific questions about their location or country of origin. **For example, if they list a university you're familiar with, ask which café on campus was their favorite.** You can also request them to say something in their native language. Many fake candidates won't be able to answer these questions, and some may even drop out of the interview right away.

TIP #14
Ask hometown/school related questions.


Strong_Ad_4 · 1y ago

What I adore are people who say their name is Gabriel Figueroa but they have such a thick Asian accent they cannot pronounce it. I also had a guy tell me he enjoyed his view of the Pacific from his balcony in Miami

Figure 13. Comment by Strong_Ad_4 under a Reddit post "Inundated with fake candidates" (2024)

Perform a **Google reverse image search** to check if the candidate's photo has been stolen from another source. Additionally, use AI-powered analysis tools to verify resumes for inconsistencies or red flags.

TIP #15
Perform a Google reverse search. on LinkedIn profile picture.

> **“[...] I feel like I’m going crazy because just about every application is a fraud when doing a little digging. I even had one LI application where the profile pic was a stock picture from Walmart ad (...).” ~ Bake-Capable**

Figure 14. Comment by Bake-Capable under a Reddit post “Inundated with fake candidates” (2024)

If a candidate is using AI to alter their audio, there may be noticeable delays or mismatches between their lip movements and spoken words. **Watch closely for any inconsistencies in synchronization.** Also, deepfake technology often adds artificial noise or subtle distortions to the audio to disguise these alterations.

TIP #16
Pay attention to lip movements and artificial audio noise.

If you work in HR, it’s a good idea to proactively **reach out to potential candidates on LinkedIn** instead of waiting for applications to come in. Direct outreach allows you to connect with skilled professionals who might not be actively job hunting but could be a great fit for your company. This approach often helps you find qualified candidates faster and gives you more control over the hiring process.

TIP #17
The old way of building human connections to search for and hire talents is more secure than relying on direct applicants.

The Internal Threat

No method is bulletproof. Consider this scenario: despite thorough security measures, a potentially untrustworthy developer is hired. In the least harmful case, they contribute nothing while continuing to receive a salary. In the worst case, they intentionally introduce vulnerabilities into the code, creating entry points for cybercriminals. **How can organizations protect themselves against this risk?**

1. Principle of Least Privilege

Limit employee access strictly to the systems and data necessary for their roles. Regularly review and adjust permissions to prevent unauthorized access and potential misuse.

2. Ongoing Security Training

Ensure employees are aware of cybersecurity risks, including social engineering tactics. Regular training helps build a security-conscious workforce that can recognize and respond to threats effectively.

3. User Activity Monitoring

Ensure employees are aware of cybersecurity risks, including social engineering tactics. Training should provide real-world context, case studies, and examples of how these attacks appear in their specific work environment.

Without real-world training, they may fail to recognize threats. With AI-enabled fraud on the rise, regular, scenario-based training is crucial. Shreem Growth Partners offers executive briefings and simulated assessments to enhance cybersecurity awareness, ensuring employees can detect and respond to attacks confidently.

4. Automated Code Security Reviews

Utilize modern security tools that leverage large language models (LLMs) to analyze code for vulnerabilities before deployment. VIDOC, for example, automates security code reviews, identifying complex vulnerabilities that could be exploited by malicious actors. It also provides insights into how much of your code is AI-generated or copied, helping maintain control over software integrity.

Summary

AI is changing the way people apply for jobs, making it easier to create resumes, cover letters, and even fake job interviews. While AI can be helpful, it also makes it easier for fake candidates to trick companies.

As technology keeps advancing, so will these scams. But by staying aware, updating hiring processes, and using both smart tools and human judgment, companies can protect themselves and find the right people for the job. Deepfake technology is improving, but there are still ways to catch it.

AI in Modern Recruitment: Avatars, Video Interviews, and Ethical Considerations

Artificial intelligence tools are reshaping high-volume recruitment processes. Video interviews are now used by approximately 75% of large organizations according to the State of Automated Interview Management 2023 report (*Phenom & Talent Board (2023)*

The State of Automated Interview Management: 2023 Survey Report. [https://assets.phenom.com/hubfs/02_Assets/ebook/230616_EB_EN_Talent-Board-Report_2023.pdf]).

AI-driven assessment layers are gaining adoption, with HR.com's 2024 Talent Acquisition Technology survey indicating **approximately 22% of organizations now use some form of AI evaluation in their screening processes.**[2] When implemented with human oversight, these systems can reduce screening time, generate structured candidate data, and standardize evaluation criteria. However, peer-reviewed evidence of bias reduction remains limited, algorithmic drift presents an ongoing risk, and the processing of GDPR-regulated biometric data requires substantial security controls.

This chapter examines the current state of practice, highlights validated implementations, distinguishes between marketing claims and proven outcomes, and provides a framework for ethical and lawful deployment.

AI Avatars in Recruitment

Recruitment avatars utilize natural language processing and supervised machine learning models to conduct structured interviews, record responses, and evaluate candidates against predetermined criteria. Some implementations feature anthropomorphic interfaces such as the Tengai robot developed by Furhat Robotics in collaboration with TNG, designed to create a more engaging candidate experience. Behind these interfaces, the technology typically includes speech recognition, sentiment analysis, and response evaluation algorithms operating within defined parameters.

The World Economic Forum has documented an early pilot implementation in Upplands-Bro, a Swedish municipality that deployed Tengai for frontline service position screening (*Bewicke H. (2019, July 18) World Economic Forum. This robot interviewer is helping Sweden recruit without bias. [https://www.weforum.org/stories/2019/07/sweden-robot-remove-bias-from-recruitment/]*). **According to the developers, the system's declared goal is to reduce unconscious bias through standardized questioning, though it is important to note that no peer-reviewed studies or published metrics currently validate these intended outcomes.** The WEF case study describes the initiative but does not provide quantitative data on bias reduction effectiveness. Technical integration occurs through standard APIs connecting to applicant tracking systems, with interview transcripts and evaluation data forwarded for human review and decision-making.

These systems offer several operational advantages. Process standardization ensures identical question wording, sequencing, and timing for all candidates, creating consistent evaluation conditions. Scalability allows parallel interview processing without scheduling constraints, enabling organizations to handle larger candidate volumes with existing resources. Structured data collection generates machine-readable response information that facilitates systematic analysis and comparison across candidate pools and over time.

Despite these benefits, documented limitations exist. Current NLP systems demonstrate reduced accuracy when processing specialized terminology, complex explanations, or non-standard speech patterns. Research in Technological Forecasting and Social Change (*Langer et al. (2021) DOI: 10.1016/j.techfore.2021.120831*) indicates mixed candidate reactions to AI interfaces in recruitment, with acceptance varying based on technological familiarity and clarity of employer communication. The NIST AI Risk Management Framework 1.0 (*NIST (2023) Artificial intelligence risk management framework (AI RMF 1.0). [https://doi.org/10.6028/NIST.AI.100-1]*) specifically highlights the risk of algorithmic bias when training data reflects historical hiring patterns or lacks sufficient diversity. A notable example of technology adaptation occurred when HireVue discontinued its facial analysis scoring features in January 2021 following criticism from the Electronic Privacy Information Center and internal review of validity evidence (*Knight W. (2021, January 12) Job Screening Service Halts Facial Analysis of Applicants. WIRED. [https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/]*).

Recorded Video Interviews & Assessment Platforms

The standard implementation workflow for recorded video interviews begins with recruiters configuring assessment batteries with timed video questions and skills evaluation modules. Candidates receive secure access links and complete technical verification to ensure their camera and microphone function properly. The system records responses asynchronously, with subsequent evaluation by hiring teams.

TestGorilla (*www.testgorilla.com*) represents a comprehensive implementation of the recorded video interview approach. **Their platform combines custom video questions with over 300 pre-validated assessment modules covering cognitive abilities, personality traits, situational judgment, language proficiency, role-specific skills, and programming capabilities.** According to their documentation, their assessment format typically combines 2 - 5 scored test modules with optional custom video questions, creating a multi-dimensional candidate evaluation in a single session.

The platform's video component allows recruiters to create personalized questions with adjustable time limits for preparation (15-120 seconds) and response (1-5 minutes). Candidates can view themselves while recording, but notably, TestGorilla permits only a single recording attempt per question to maintain assessment integrity. For security purposes, the system captures webcam snapshots every 30 seconds during the assessment (*TestGorilla (2025) Understanding anti-cheating measures. [https://support.testgorilla.com/hc/en-us/articles/9028797639451-Understanding-anti-cheating-measures]*), logs IP addresses, and monitors tab-switching behavior.

TestGorilla's implementation differentiates itself through its "blind hiring" approach, which presents assessment scores to recruiters before revealing candidate identifying information, a feature designed to reduce initial screening bias. Their case study reported **reducing time-to-hire by 34% with an average time-to-hire of 29 days for technical roles** (*TestGorilla (n.d.) Skills-First Hiring: Key Takeaways. [https://www.testgorilla.com/case-studies/testgorilla-cuts-hiring-time-by-evaluating-skills-first/?_gl=1*1gzp4po*_up*MQ..*_gs*MQ..*_ga*MjA4MzM5MzgxMy4xNzUxMzUzNjk3*_ga_R6DQ0KX3NX*czE3NTEzNTM2OTckbzEkZzAkdDE3NTEzNTM2OTckajYwJGwwJGgxOTkxNDg4NDEx&gclid=Cj0KCQjwjo7DBhCrARIsACWauSmd2SOOInlqi49izaH_atDWRGMNfqPrmh27nLRXWetKn56RRWwhGMgaAlhcEALw_wcB&gbraid=0AAAAABnxgtApCOyVX6RKr4KyJi5CqhIJt]*).

Vodafone's enterprise implementation provides valuable insights into large-scale deployment. According to a case study published by Sova Assessment (*Sova Assessment (2022) How Vodafone implemented a fair global hiring process while driving down technology costs. [https://www.sovaassessment.com/customer-stories/vodafone]*), they processed approximately 65,000 candidates in six months across graduate and retail recruitment programs. **Their hybrid approach combined automated initial screening with human validation of results, achieving a Net Promoter Score of +44 from candidates while reducing recruiter time per application by approximately 50%.**

Unilever has also documented efficiency gains through their video assessment implementation. In 2017, Unilever set a target of reducing their graduate recruitment timeline from approximately four months to around two weeks (Raphael *T. (2017) Unilever Wants to Shorten Hiring From 4 Months to 2 Weeks. ERE. [https://www.ere.net/articles/unilever-wants-to-shorten-hiring-from-4-months-to-2-weeks]*). While follow-up studies don't confirm this exact timeline reduction, The Guardian (*The Guardian (2019) Unilever saves on recruiters by using AI to assess job interviews. [https://www.theguardian.com/technology/2019/oct/25/unilever-saves-on-recruiters-by-using-ai-to-assess-job-interviews]*) later reported that their **AI-assisted recruitment process saved an estimated 100,000 work hours of recruiter time while increasing diversity in their**

entry-level hiring. The implementation of video interview systems creates specific risk considerations that organizations must address. The following risk assessment matrix outlines key vulnerabilities and recommended controls:

Risk domain	Typical vulnerability	Recommended controls
Data Privacy (GDPR Art. 9)	Processing biometric data without appropriate legal basis	Implement explicit consent mechanisms (as "legitimate interest" is insufficient for biometric data); establish maximum 12-month retention policy with automated deletion
Information Security	Unauthorized access to interview recordings	Deploy ISO/IEC 27001:2022-compliant access controls with comprehensive audit logging
Identity Verification	Deepfake impersonation or proxy test-taking	Implement liveness detection; require multi-factor authentication; conduct manual ID verification for final candidates
Assessment Integrity	AI-assisted cheating on technical evaluations	Utilize dynamic question pools; deploy plagiarism detection; implement keystroke analysis

Compliance & Ethical Framework

Organizations implementing AI recruitment technologies must navigate a complex regulatory landscape. The European Data Protection Board Guidelines 3/2019 clarify that biometric data collected during video interviews falls under GDPR Article 9's special category protections, requiring explicit consent for processing. Organizations cannot rely on legitimate interest as a legal basis for processing this type of data, making clear consent mechanisms essential.

The NIST AI Risk Management Framework 1.0 (2023) provides comprehensive guidance on managing AI risks, including specific considerations for bias mitigation, explainability standards, and validation controls. Similarly, the European Union Agency for Cybersecurity (ENISA) publication "Securing Personal Data in the Wake of AI" (*European Union Agency for Cybersecurity (2023) Securing Personal Data in the Wake of AI. [http://enisa.europa.eu/news/securing-personal-data-in-the-wake-of-ai]*) recommends conducting data protection impact assessments before system launch and implementing continuous monitoring throughout the technology lifecycle.

Transparency forms the foundation of ethical AI implementation in recruitment. Organizations should inform candidates clearly about how AI is used in the process, what data is captured, how long it will be retained, and who makes final decisions. Best practices include providing a detailed FAQ page with sample assessment questions and offering a non-AI alternative pathway to accommodate candidates with accessibility needs or specific concerns about AI evaluation.

Technical safeguards for securing video interview data should align with established information security frameworks. The Cloud Security Alliance identifies mutual TLS encryption for data in transit, SOC 2 Type II certified hosting environments, role-based access controls implementing the principle of least privilege, comprehensive audit logging with tamper-evident records, and automated data deletion protocols as recommended protective measures for biometric data (*CSA (2024) Cloud Controls Matrix and CAIQ v4. [https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4]*).

Effective bias monitoring requires a systematic approach implemented throughout the system lifecycle. **Before launch, organizations should test the assessment platform with representative datasets and document performance parity across demographic groups.** Quarterly reviews should compare pass rates by gender, age, ethnicity, and other protected characteristics, with variances greater than 4% triggering investigation and potential adjustment. When algorithm retraining occurs, comprehensive validation and version control ensure that improvements can be properly documented and verified.

Practical Implementation Model

Organizations achieving sustainable results typically implement a **hybrid approach that combines AI efficiency with human judgment**. The initial stage utilizes avatar-based or asynchronous video interviews with AI scoring to efficiently process large candidate pools. A critical human review gate follows, where recruiters evaluate top-performing candidates as well as borderline cases (typically those scoring between 40-60% on automated assessments). **This ensures that algorithmic assessments don't inadvertently eliminate qualified candidates.** The process continues with live interviews focused on competency verification and cultural fit assessment conducted by hiring managers. Finally, the offer and onboarding stage can integrate insights from the assessment process to inform personalized training and development plans.

Benchmark data from published case studies indicates that effectively implemented systems can improve recruitment efficiency. **TestGorilla's customer data shows time-to-hire reductions of 34%** (*TestGorilla case study*), **while Sova Assessment reports roughly**

50% reductions in recruiter time per candidate (*Vodafone case study*). Candidate satisfaction scores typically reach favorable levels when organizations provide transparent information about the process and assessment criteria, with Vodafone's implementation achieving a Net Promoter Score of +44 from candidates.

The technical implementation of AI cheating detection has become increasingly important as generative AI tools advance. **Organizations must address the growing challenge of AI-assisted responses in technical assessments**, though public metrics on prevalence remain limited. According to industry practitioners, assessment platforms have been enhancing their detection capabilities as candidates increasingly attempt to use language models during coding tests and other technical evaluations. CoderPad's blog (*CoderPad's blog (2025) Cheating Prevention and Detection. [https://coderpad.io/resources/docs/screen/tests/cheating-prevention-detection/]*) has documented this trend, noting that detection capabilities now include keystroke analysis, coding pattern recognition, and comparative analysis of candidate solutions against known AI-generated patterns.

Research on candidate acceptance of AI interfaces has yielded valuable insights for implementation. Studies in the field of human-computer interaction highlight that transparency about assessment criteria significantly influences candidate perceptions. A study by Langer et al. in Computers in Human Behavior (*Langer et al. (2023) Computers in Human Behavior. [https://www.sciencedirect.com/science/article/pii/S2451958823000362?via%3Dihub]*) examined reactions to automated interview systems, finding that perceived fairness and procedural transparency were key determinants of candidate acceptance.

Figure 15. Organizations must address the growing challenge of AI-assisted responses in technical assessments

Key Recommendations

Organizations implementing AI recruitment technologies should start with small-scale pilots focused on high-volume roles where standardized evaluation criteria can be clearly defined. Baseline metrics should be established before implementation to enable meaningful comparison and ROI evaluation. Human oversight must remain central to the process, with AI systems assisting rather than replacing human decision-makers. This maintains accountability while leveraging technological efficiency.

Transparency should be prioritized through dedicated informational resources that explain the assessment process, provide sample questions, and clarify how AI is used in evaluation. **Regular bias and security audits should occur at least quarterly to identify and address potential issues before they affect hiring outcomes.** Organizations should also plan for digital divide considerations by providing alternative access options, such as in-store kiosks for retail positions or low-bandwidth assessment paths for candidates with limited internet connectivity.

Conclusion

AI avatars and video interviews represent significant developments in recruitment technology with potential benefits for efficiency, objectivity, and candidate experience. **However, successful implementation requires addressing technical limitations, candidate acceptance factors, potential biases, and privacy concerns through thoughtful system design and ongoing monitoring.**

Organizations should approach these technologies with a balanced perspective, implementing appropriate safeguards while leveraging potential benefits. A hybrid approach that combines AI efficiency with human judgment will typically yield optimal results, creating more effective recruitment processes while maintaining necessary human involvement in hiring decisions.

As these technologies continue evolving, implementation decisions should align with specific recruitment needs, organizational values, regulatory requirements, and candidate expectations. When integrated into carefully designed processes with appropriate controls, these tools can enhance recruitment effectiveness while treating candidates with fairness and respect.

Background check of future employees. How do you do that?

With competition growing and security concerns on the rise, more and more companies are paying close attention to the risks that come with hiring. **A bad hire can lead to legal trouble, financial loss, or even damage a company's reputation.** That's why background checks have become such an important part of the hiring process — they help create safer, more reliable teams and give companies peace of mind when bringing someone new on board.

TIP #18
In 2021, 91% of organizations conducted background screening for full-time employees.

Why Background Checks Matter

If you want to be confident about who you're hiring, running a background check is a smart move. Many large companies, from Microsoft to Meta, treat background screening as a standard part of their hiring process — not just for full-time roles, but also for interns and contractors. It's a core part of building safe, trustworthy, and high-performing teams.

Among the companies known for taking background checks seriously are:

- Microsoft
- Google
- Amazon
- Apple
- IBM
- Meta (Facebook)
- Accenture
- Deloitte
- KPMG
- Ernst & Young (EY)
- PwC

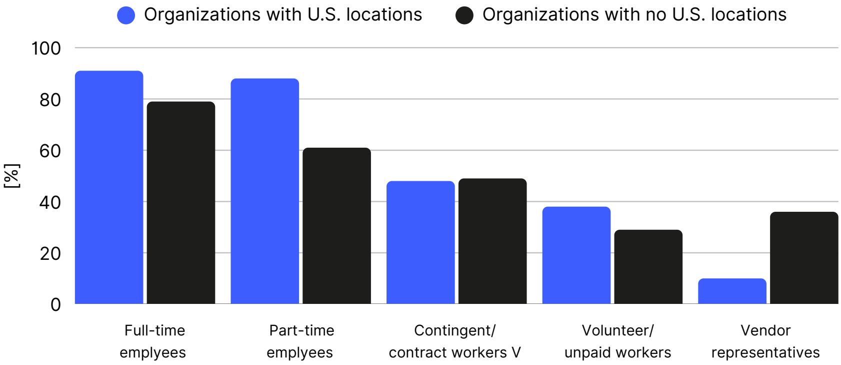


Figure 16. How often employers conduct background checks based on type of employment by HR Research (2021)

These organizations use pre-employment screening to reduce risks — legal, financial, or reputational — and to ensure that new hires meet their internal standards of integrity and reliability.

What Does a Background Check Include?

Pre-employment screening can cover many areas, depending on the company, role, and local laws. Common types of checks include:

1. Academic Verification
Ensuring degrees or certifications are real.

2. Character References
Contacting past supervisors or colleagues.

3. Employment History Gaps
Investigating any breaks in employment.

4. Education Gaps
Checking for consistency in education records.

5. Identity and Address Verification
Confirming the candidate's identity and residence.

6. Additional Risk Checks
In some cases, screening may also include anti-money laundering, terrorism lists, or passport validation.

Before any check is conducted, the candidate must give written permission. In most cases, this happens during the offer stage. The HR or staffing representative usually informs the candidate of the screening requirements when the offer is extended.

Who Performs the Checks?

Many companies work with trusted background check providers to manage the process efficiently and stay compliant with the law. Here are some of the most widely used services:

- **HireRight** – Global background checks and drug testing.
- **Checkr** – AI-powered checks, used by companies like Uber.
- **Sterling** – Full-service screenings for companies of all sizes.
- **GoodHire** – Flexible and industry-specific solutions.
- **First Advantage** – Compliance-focused screening with global reach.

These services make it easier for companies to make informed, confident hiring decisions — while also protecting candidate privacy and following all necessary legal requirements.

The Purpose of Pre-Employment Screening

The goal of pre-employment checks isn't just about checking boxes — it's about building trust. Here's what companies aim to confirm:

1. **That the candidate is who they claim to be.**
2. **That they are legally allowed to work in the country** (e.g. EU, US, UK).
3. **That nothing in their past work history raises red flags for the new role** (e.g. serious misconduct, unresolved HR issues).
4. **That they actually have the qualifications, skills, and experience they listed.**
5. **That there are no health or personal issues that would prevent them from doing the job safely or effectively.**

Even without a large HR department or budget, understanding how background checks work — and how to conduct them legally and ethically — can help small companies hire with confidence. In the next section, I'll walk you through how we do this in practice, even without using external providers.

What About Small Companies Without a Budget?

I checked that the cost of one limited background check starts at $30. It's not a significant expense, but as mentioned, it's limited — additional criminal checks cost extra.

Hiring can be especially challenging for small companies with limited resources. Without access to expensive recruitment platforms or professional background-check services, you need a smart, lean, and legally compliant approach.

Let me share how we do it at our company.

Step 1: LinkedIn Screening

Before scheduling any interview, I always check the candidate's LinkedIn profile. First, I verify if the profile looks real and complete — fake profiles are unfortunately common, especially in tech. We discussed this in more detail in the previous chapter of this guide.

I look for:

- A consistent job history and education timeline
- Confirmed connections and mutual contacts

- Engagement in the community (posts, comments, recommendations)

If everything looks solid, I move to the next step.

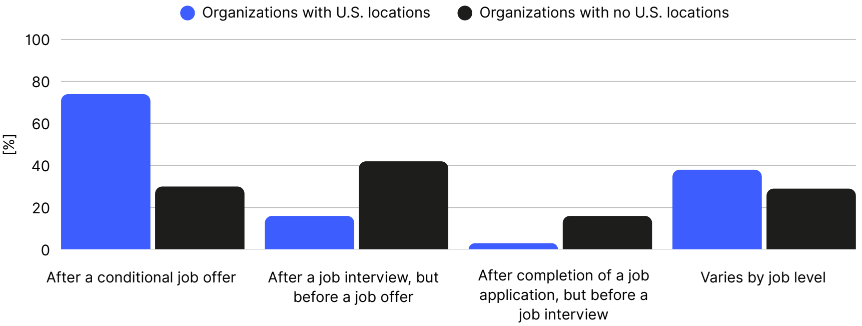


Figure 17. At what point during the hiring/onboarding process does your organization typically conduct background screening? By HR Research (2021)

Step 2: Verifying Work History

During or after a few online interviews, I ask the candidate to provide a reference contact — ideally, a direct manager — from two or three of their previous employers. These companies are selected by me based on the candidate's experience.

In the European Union, GDPR regulations limit how we can share or collect personal data during the recruitment process. This means traditional third-party background checks (like those used in the U.S.) are often not allowed without clear consent. Instead, we ask the candidate for permission to contact specific people — this keeps the process both ethical and legal.

According to the European Commission, consent must be freely given, specific, informed, and unambiguous (*Article 4(11), GDPR*), so make sure you're clear with candidates about what data you'll collect and how you'll use it.

Step 3: In-Person Interview

Once the reference check is complete, we invite the candidate for an on-site meeting (when possible). This gives us a chance to get to know the person beyond the screen and evaluate how they might fit into the team environment.

Tips for Other Small Companies

If you're a startup or small business, here are a few tips from industry experts:

- Use your network: Ask current employees to refer candidates. Referred hires often perform better and stay longer.
- Get creative with sourcing: Participate in open-source communities, local tech meetups, and job boards.
- Be transparent: Candidates appreciate honesty about your stage and limitations. Sell them on the mission, not the money.

Document your process: It shows professionalism and helps protect you legally.

The Background Check – More Than a Checkbox

There was a time when background checks were nothing more than a quick administrative routine — just another box to tick off before signing the contract. But those days are long gone. In today's workplace, background checks have quietly evolved into something far more important: a moment that can shape how employees feel about your organization right from the start.

It turns out, **how you *check* says a lot about how you *trust*.** When companies approach background screening with transparency and fairness, it helps build a culture of respect. This isn't just about finding red flags — it's about showing potential employees that you believe in second chances, fairness, and treating people like, well... people. When candidates feel like they're being judged fairly — and have a chance to explain any grey areas — they're more likely to trust the company, feel engaged, and stick around for the long haul.

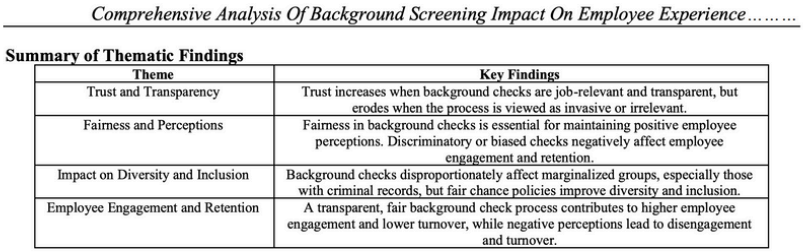
87% **Of employers do background checks during the pre-employment stage.**

(shrm.org, 2025)

This sense of fairness also ties directly into employee satisfaction and retention. If the process feels clear, job-relevant, and free from bias, people don't walk away with a sour taste in their mouth. In fact, they feel more connected. Fair checks help preserve their dignity and reinforce a message: "We trust you, and we see you as a whole person."

And then there’s the impact on diversity and inclusion. If background checks are too rigid or lack context, they can unintentionally exclude candidates from underrepresented or historically marginalized communities. That’s a missed opportunity — both ethically and strategically. But when companies implement inclusive, thoughtful screening practices — such as fair chance hiring — they create space for diverse talent to thrive. These organizations don’t just talk about inclusion; they practice it from the very first interaction.

Lastly, let’s not forget the effect on overall workplace morale. A background check process that is consistent, fair, and respectful sets the tone for the entire employee experience. It signals that the company cares — not just about rules and risk — but about people. **And when people feel respected from day one, they’re more likely to give that respect back.**



Comprehensive Analysis Of Background Screening Impact On Employee Experience………

Summary of Thematic Findings

Theme	Key Findings
Trust and Transparency	Trust increases when background checks are job-relevant and transparent, but erodes when the process is viewed as invasive or irrelevant.
Fairness and Perceptions	Fairness in background checks is essential for maintaining positive employee perceptions. Discriminatory or biased checks negatively affect employee engagement and retention.
Impact on Diversity and Inclusion	Background checks disproportionately affect marginalized groups, especially those with criminal records, but fair chance policies improve diversity and inclusion.
Employee Engagement and Retention	A transparent, fair background check process contributes to higher employee engagement and lower turnover, while negative perceptions lead to disengagement and turnover.

Figure 18. Key Themes and Findings From Princewill’s “Comprehensive Analysis of Background Screening Impact on Employee Experience” (2024)

What’s The Takeaway?

The background check isn’t just a legal hurdle or a formal step — it’s a first impression. Get it right, and you build trust, loyalty, and a stronger, more inclusive team. Get it wrong, and you might lose great people before they even start.

A large percentage of employers perform background checks during the recruitment process. For instance, **Uber takes 3 to 5 business days to review an applicant’s records.** Before hiring, companies employ checks to evaluate candidates’ qualifications, past work experiences, and criminal history.

Legal Responsibility

Using a fake identity during the recruitment process can lead to various legal consequences, depending on the nature of the actions, underlying intent, and potential outcomes.

From a criminal law perspective, in Poland, charges may include fraud (punishable by up to 8 years imprisonment), document forgery (punishable by up to 5 years imprisonment), or public use of titles or degrees to which one is not entitled (punishable by fine or reprimand). Impersonating a real person by using their image, personal data, or other identifying information is punishable by up to 8 years imprisonment.

In the United States, **individuals using fake identities can be prosecuted under federal identity theft and fraud statutes, with penalties that can include up to 20 years imprisonment.** Each state may also have its own statutes.

Additional charges may apply when fake identity schemes target corporate espionage or infiltration of company systems. Law enforcement agencies warn that fraudsters frequently target remote IT positions with access to customer personal data, financial information, or trade secrets (*Federal Bureau of Investigation (2022, June 28) FBI warns of fraudulent employment ads. IC3.gov. [https://www.ic3.gov/PSA/2022/psa220628]*).

Those using fake identities bear civil liability both to the defrauded company and the person they impersonated. Companies may seek damages for recruitment costs incurred, losses from hiring unqualified personnel, lost profits, and costs associated with detecting and reversing fraud consequences. The impersonated individual may pursue compensation for violations of personal rights and damage remediation. In common law systems, civil claims are also possible, with grounds depending on specific circumstances.

Companies may face liability if they fail to meet appropriate verification standards, particularly for sensitive positions such as those involving access to confidential data, financial information, or significant responsibility.

In the United States, employers have a legal obligation to verify identity and work authorization for every employee through Form I-9 (Employment Eligibility Verification) (*U.S. Citizenship and Immigration Services. (n.d.). Statutes and regulations. I-9 Central. [https://www.uscis.gov/i-9-central/form-i-9-resources/statutes-and-regulations]*).

Companies should document their recruitment procedures and apply them consistently, adjusting their scope based on risk. Regular HR team training, creating verification checklists, and working with legal departments when designing recruitment processes constitute basic protective measures.

Figure 19. Companies can claim costs from fraud, including hiring losses and profit damage

When fraud is detected, swift action, comprehensive incident documentation, and cooperation with law enforcement are crucial, as these may demonstrate employer good faith. Delays can be costly since fake identity fraudsters typically conceal their real identities and may quickly eliminate evidence.

Report

When identity fraud is detected, specific reporting obligations may arise.

Reporting to law enforcement can be accomplished through:
1) In Poland – reporting to police station,
2) In the United States – reporting via the Internet Crime Complaint Center (*https://www.ic3.gov/*) or contacting the local FBI field office.

If the individual gained access to other individual's personal data, there may be an obligation to report the breach to supervisory authorities (*in Poland – Personal Data Protection Office, https://www.uodo.gov.pl/en/p/contact*). Social media platforms like LinkedIn take action to ensure authenticity. Report fake profiles and content directly to the platform through dedicated channels. It's important to secure evidence before reporting in a form that can serve as proof in criminal or civil proceedings (including screenshots, HTML page saves). While platforms temporarily retain deleted data, law enforcement have to provide specific details to obtain access to it.

Victim notification is both good practice and may be legally required. In the EU under Article 14 GDPR, data controllers must inform individuals within one month about data sources, unless this proves impossible or disproportionately difficult.

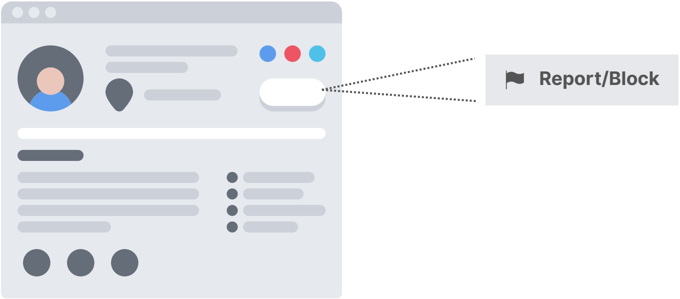


Figure 20. Report fake accounts directly on the social media platform. It's the first step to stopping fraud

Public Disclosure

Priority should be protecting the person who was impersonated – notifying them and securing their interests – and taking appropriate action against the person responsible. The recommended approach includes:

- Communicating about fraud methods without revealing the victim's personal data or other identifying information,
- Using industry HR forums to share anonymized fraud patterns,
- Cooperating with law enforcement agencies that can coordinate actions.

Legal Restrictions on Biometric Use

When using biometric technology for candidate verification, remember that it may be subject to strict legal regulations in some jurisdictions, including employment law, data protection regulations, and AI use requirements.

In the EU, biometric data is considered a special category of personal data with restricted processing requirements. It is generally prohibited unless one of the specific exceptions applies, such as explicit consent. In the United States, regulations vary by state – written may be required before collecting biometric data, and some practices may be considered privacy violations.

Given this complex regulatory landscape, adopting data protection by design principles is recommended. This proactive approach helps companies minimize data breach risks and build candidate trust while preparing for potential changes in privacy regulations.

Companies should monitor regulatory changes and adapt their procedures to the evolving legal and technological landscape. Due to differences in legal systems or authority approaches, specific strategies should be discussed with local legal counsel.

Figure 21. Exposing fraud starts with protecting the victim

Informing candidates about data processing principles and AI system use may be legally required and can also help deter potential fake candidates from applying. However, implementing advanced verification systems should never replace the need to stay alert.

Cheat-Sheet: Hiring in the Era of AI Deepfakes

Short summary for busy HR professionals, recruiters, and hiring managers.

1. Conduct Basic Verification Early

- Request official IDs (where legal).
- Check LinkedIn & social media activity.
- Do quick open-source intelligence (OSINT): Google reverse image search on candidate photos.

🚩 **Red flags:**

brand-new profiles, missing or AI-ish photos, suspiciously generic posts, high number of followers with no posts.

2. Require Live Video (and Record It)

Politely inform candidates that the interview will be recorded (with jako clear and freely given consent).

- Observe real-time facial expressions and audio sync-deepfake distortions often slip under repeated viewing.
- Ask for movements that disrupt deepfakes (e.g., covering part of the face, turning head).

3. Check Consistency Across Interviews

- Repeat certain questions in multiple rounds; watch for drastically different answers/accents.
- Evaluate posture, accent, and spontaneous replies. Overly polished “ChatGPT style” bullet points may signal AI scripting.

4. Ask “Hometown / Alma Mater” Questions

- If they claim a certain school, ask about a well-known café on campus.
- Request a short phrase in their native language.
- Fake candidates often stumble or disconnect.

5. Scrutinize Background & References

- Cross-check work experience details. Strange combinations (e.g., “Meta + random university from the other side of the world + broken English”) need deeper investigation.

- Call references from previous employers; verify position, responsibilities, and identity.
- Watch out for “stacked” remote jobs: some fake hires juggle multiple roles for quick pay or data theft.

6. Encourage On-Site or Hybrid Interviews

- Budget allowing, finalize hires with an in-person day.
- If international travel is tricky, partner with local co-working spaces or branch offices for real-world meetups.

7. Legal & Security Measures

- Inform candidates that impersonation is a serious offense; mention you record interviews for compliance.
- Keep IT involved: suspicious software or remote access flags should trigger deeper background checks.
- Maintain logs of IP addresses or unusual login times if using remote coding tests.
- Evaluate risks and determine which positions need extra verification, e.g. face-to-face meetings or double-checking procedures.
- Ensuring up-to-date incident response procedures.
- Securing digital evidence in a manner that ensures data integrity.

8. Red-Flag Behaviors

- Camera “broken” multiple times.
- Overly scripted or unnatural responses (AI-generated feel).
- Delayed or robotic audio (possible voice modulation software).
- No social footprint except a bare LinkedIn profile.

9. Share Knowledge Internally

- Train HR teams and managers to spot deepfake signs.
- Circulate real examples of AI-assisted fraud among staff.
- Encourage employees to report suspicious interactions.

10. Evolve & Adapt

- As AI tech improves, so should your screening methods.
- Use or build AI tools that analyze micro-expressions or detect oddities in real-time.
- Update policies—regularly remind recruiters about new AI scams.

Stay sharp. Keep refining. Don’t let AI-driven fraudsters hijack your hiring process.

Meet Our Authors

Klaudia Kloc

The CEO and co-founder of Vidoc Security Lab, a company that develops AI-powered solutions for detecting and fixing security vulnerabilities in complex software systems. An expert in offensive security and AI, she has ethically hacked major tech companies like Yahoo, Microsoft, and Uber. She also works with NGOs on digital safety and speaks at tech conferences.

Dawid Moczadło

The CTO and co-founder of Vidoc Security Lab, a cybersecurity startup that raised $2.4M from leading Silicon Valley VCs. Featured on Forbes '30 Under 30' and recognized by Microsoft as a top ethical hacker in 2021, he has discovered critical vulnerabilities in major tech companies including Meta, PayPal, and more. He regularly speaks at cybersecurity conferences

Zuzanna Mówińska

Zuzanna Mówińska is a UX/UI and Creative Designer at Vidoc Security Lab, where she also leads social media and supports marketing efforts. A designer by passion, she enjoys hacking algorithms in her free time and is deeply interested in privacy and security topics.

Paulina Michalczyk

The Head of Operations at Vidoc Security Lab, where she drives efficiency, strategic growth, and team alignment. Before joining the startup world, she successfully managed two public sector facilities. Paulina brings a strong commitment to innovation, structure, and impactful leadership.

Monika Kamińska

CEO and founder of Truesty, a legal-tech startup removing illegal and harmful online content – from fake reviews to deepfakes – before it harms reputations. An attorney with 10+ years' experience shaping national and EU regulations, she turns complex law into fast, ethical digital protection for individuals, VIPs, brands, and institutions.

Piotr Brzyski

The founder of ZetaTech and a member of GRAI - AI advisors group to the Polish Ministry of Digital Affairs. He leads the AI_Devs community of 4,000+ developers and focuses on practical AI implementation while maintaining a critical perspective on the technology's real-world limitations.

Sources

Articles:

- Lyons, J. (2025, February 11). *I'm a security expert, and I almost fell for a North Korea-style deepfake job applicant … twice.* The Register. [https://www.theregister.com/2025/02/11/it_worker_scam].
- Sjouwerman, S. (2024, October 19). *How a North Korean Fake IT Worker Tried to Infiltrate Us.* KnowBe4. [https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us].
- Naraine, R. (2024, December 12). *Fake IT Workers Funneled Millions to North Korea, DOJ Says.* Security Week. [https://www.securityweek.com/fake-it-workers-funneled-millions-to-north-korea-doj-says/].
- Park, S. (2024, November 4). *From Pyongyang to Your Payroll: The Rise of North Korean Remote Workers in the West.* Zscaler Blog. [https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west].
- Archives U.S. Department of Justice (2025, February 6) *Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator.* [https://www.justice.gov/archives/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and].
- da Silva, J. (2024, December 20). *N Korea hackers stole $1.3bn of crypto this year - report.* BBC. [https://www.bbc.com/news/articles/cwy3dz0614jo].
- Thakur, S. (2016). *Pre-Employment Screening: Advantages and Disadvantages.* Indian Journal of Research, 5(8), 185-186 [www.worldwidejournals.com/paripex/recent_issues_pdf/2016/August/preemployment-screening-advantages-and-disadvantages_August_2016_0924156920_5306646.pdf?utm_source=chatgpt.com]
- H. M. Nadim Khan, Md Sajjad Hosain, Hasina Imam October 2024 Journal of Business Sectors 2(2):31-39 *Pre-employment background check: A review and research agenda [https://www.researchgate.net/publication/385291445_Pre-employment_background_check_A_review_and_research_agenda]*
- Hosain, M. S., & Liu, P. (2019). *Conducting pre-employment background checks through social networking sites: The new role of HR professionals.* Journal of Economics, Management and Informatics, 10(2), 111–123.
- Princewill, A. O. (2024). *Comprehensive analysis of background screening impact on employee experience and organizational outcomes.* IOSR Journal of Economics and Finance (IOSR-JEF).
- Lopez, J. (2024, September 3). *Human Firewall: How Employees Can Protect or Compromise a Company's Cybersecurity.* DevX. [https://www.devx.com/web-development-zone/human-firewall-how-employees-can-protect-or-compromise-a-companys-cybersecurity/]
- Archambault, S. (2025, May 23). *Top 15 Best Background Check Services in 2025.* GoodHire. [https://www.goodhire.com/resources/articles/best-background-check-services/?utm_source=chatgpt.com].

Footnotes

[1] Screenshoted articles

Scanned articles were used as reference material in the creation of this ebook. Therefore, they are listed under the Articles section to ensure source transparency and traceability.

[2] Some industry analysts report higher adoption rates in private, subscription-based research. For example, Gartner's 2024 HR Technology Survey (available only to subscribers) suggests figures around 27% for enterprise organizations specifically.

Other links:

- Lewis, L. (2021, October 14). *2021 Hiring Trends Report.* Indeed For Employers. [https://www.indeed.com/lead/2021-hiring-trends-report?hl=en&co=US].
- *Introducing ChatGPT. (2022, November 30).* Open AI. *[https://openai.com/index/chatgpt/]*.
- *Artificial intelligence.* (2025, May 29). Wikipedia. [https://en.wikipedia.org/wiki/Artificial_intelligence]. (Access: February 27, 2025).
- Ruczynski, K. (2025, February 12). *AI x Hiring*. AI + consumer. [aiconsumer.substack.com/p/ai-x-hiring].
- Moczadło, D. (2025, February 4). *WTF, developer used AI to alter his appearance during a technical interview with me* [Post]. Linkedin. [https://www.linkedin.com/posts/dawid-moczadlo_wtf-developer-used-ai-to-alter-his-appearance-activity-7292604406464671744-T_Nw?utm_source=share&utm_medium=member_desktop&rcm=ACoAADDK67ABbIoPW6i73iOC9kHUsjS9sjuesyw (Access: 2025, February 17).
- @Bake-Capable. (2024, March 15). *Inundated with fake candidates*. Reddit. [https://www.reddit.com/r/recruiting/comments/1bffeiu/inundated_with_fake_candidates/?rdt=34969]. (Access: 2025, March 4).
- Wikipedia (2025, May 8) *Open-source intelligence*. [en.wikipedia.org/wiki/Open-source_intelligence]. (Access: February 20, 2025).
- BeFunky. (n.d.) *Enhance Portrait Photos With a Single Click*. Retrieved: 2025, February 27 from [www.befunky.com/features/portrait-enhancer]. Note: The title and content of the page have changed since the time of access.
- Froehlich, A. (2024, May 7). *How to detect deepfakes manually and using AI.* TechTarget. [www.techtarget.com/searchsecurity/tip/How-to-detect-deepfakes-manually-and-using-AI].
- Phenom & Talent Board (2023) *The State of Automated Interview Management: 2023 Survey Report.* [https://assets.phenom.com/hubfs/02_Assets/ebook/230616_EB_EN_Talent-Board-Report_2023.pdf]
- Bewicke H. (2019, July 18) World Economic Forum. *This robot interviewer is helping Sweden recruit without bias.* [https://www.weforum.org/stories/2019/07/sweden-robot-remove-bias-from-recruitment/]
- Langer et al. (2021) What Do *We Want From Explainable Artificial Intelligence (XAI)*. [DOI: 10.1016/j.techfore.2021.120831]
- NIST (2023) *Artificial intelligence risk management framework* (AI RMF 1.0). [https://doi.org/10.6028/NIST.AI.100-1]
- Knight W. (2021, January 12) *Job Screening Service Halts Facial Analysis of Applicants.* WIRED. [https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/]
- TestGorilla (2025) *Understanding anti-cheating measures.* [https://support.testgorilla.com/hc/en-us/articles/9028797639451-Understanding-anti-cheating-measures]
- *T*estGorilla (n.d.) *Skills-First Hiring: Key Takeaways.* [https://www.testgorilla.com/case-studies/testgorilla-cuts-hiring-time-by-evaluating-skills-first/?_gl=1*1gzp4po*_up*MQ..*_gs*MQ..*_ga*MjA4MzM5MzgxMy4xNzUxMzUzNjk3*_ga_R6DQ0KX3NX*czE3NTEzNTM2OTckbzEkZzAkdDE3NTEzNTM2OTckajYwJGwwJGgxOTkxNDg4NDEx&gclid=Cj0KCQjwjo7DBhCrARIsACWauSmd2SOOInlqi49izaH_atDWRGMNfqPrmh27nLRXWetKn56RRWwhGMgaAlhcEALw_wcB&gbraid=0AAAAABnxgtApCOyVX6RKr4KyJi5CqhIJt]

- Sova Assessment (2022) *How Vodafone implemented a fair global hiring process while driving down technology costs.* [https://www.sovaassessment.com/customer-stories/vodafone]
- Raphael T. (2017) *Unilever Wants to Shorten Hiring From 4 Months to 2 Weeks.* ERE. [https://www.ere.net/articles/unilever-wants-to-shorten-hiring-from-4-months-to-2-weeks]
- The Guardian (2019) *Unilever saves on recruiters by using AI to assess job interviews.* [https://www.theguardian.com/technology/2019/oct/25/unilever-saves-on-recruiters-by-using-ai-to-assess-job-interviews]
- *European Union Agency for Cybersecurity (2023) Securing Personal Data in the Wake of AI.* [http://enisa.europa.eu/news/securing-personal-data-in-the-wake-of-ai]
- CSA (2024) *Cloud Controls Matrix and CAIQ v4.* [https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4]
- CoderPad's blog (2025) *Cheating Prevention and Detection.* [https://coderpad.io/resources/docs/screen/tests/cheating-prevention-detection/]
- Langer et al. (2023) *Computers in Human Behavior.* [https://www.sciencedirect.com/science/article/pii/S2451958823000362?via%3Dihub]

Data*:*

- Semrush. (2025, March 6). *Chatgpt.com overview.* Retrieved May 30, 2025, from [https://www.semrush.com/website/chatgpt.com/overview].
- Tidio. (n.d.). *AI recruitment statistics: What is the future of hiring?* Retrieved March 6, 2025, from [https://www.tidio.com/blog/ai-recruitment].
- IBM. (2024). *Cost of a data breach report 2024.* Retrieved March 6, 2025, from [https://www.ibm.com/reports/data-breach].

Law*:*

- Federal Bureau of Investigation (June 28, 2022) *FBI warns of fraudulent employment ads.* IC3.gov. [https://www.ic3.gov/PSA/2022/psa220628)]
- U.S. Citizenship and Immigration Services. (n.d.). *Statutes and regulations.* I-9 Central. [https://www.uscis.gov/i-9-central/form-i-9-resources/statutes-and-regulations]

Data sources methodology note:

[Specifically for chapters: AI in Modern Recruitment: Avatars, Video Interviews, and Ethical Considerations; AI Avatars in Recruitment; Recorded Video Interviews & Assessment Platforms; Compliance & Ethical Framework; Practical Implementation Model; Key Recommendations; Conclusion]

These chapters draw on multiple data sources with varying levels of public accessibility:

1. Publicly available research and reports: all sources with direct URLs provided are freely available and can be accessed by readers for verification purposes.
2. Subscription-based industry research: some figures (noted with footnotes) come from analyst firms like Gartner that provide detailed statistics only to subscribers. Where possible, alternative public sources are provided.
3. Vendor case studies: implementation examples and metrics are primarily sourced from publicly available case studies published by technology providers and their clients, which may present favorable results.

4. Peer-reviewed academic research: all academic studies are cited with DOIs to facilitate verification of research methodology and findings.

Where definitive public data is unavailable, this is explicitly noted to distinguish between established facts and areas requiring further research.

References:

- Cabala A. (2025) *4 years ago we were working with Chinise guys that stole EU identities. They were good, but apparently noticed it by coming in odd hours and always working via U.S. vpn, that pushed us to reach out real identity owner on social media. They then confessed on buying it on darkweb. I could expect something similar here.* Comment on LinkedIn post by D. Moczadło. LinkedIn [https://www.linkedin.com/posts/dawid-moczadlo_wtf-developer-used-ai-to-alter-his-appearance-activity-7292604406464671744-T_Nw/]
- Lima M. (2025) *Last month I've interviewed a Chinese that was pretending to be Brazilian so he could tryout for a LATAM only position. The first clue was he refusing to speak one word in portugese. Also his english accent was also giving him up.* Comment on LinkedIn post by D. Moczadło. Linkedin [[https://www.linkedin.com/posts/dawid-moczadlo_wtf-developer-used-ai-to-alter-his-appearance-activity-7292604406464671744-T_Nw/]
- hankmardukas66 (2024) *Check their connections on LinkedIn, often they'll have very few and they're all recruiters. Look for connections at the company they claim to work at, often they'll claim to work at massive companies because it's harder to catch the lige but they should still have connections. Ask them straight up for a referral from their team before booking a call at all (they'll likely ghost). I tell them straight up it's a verification method because we get a lot of fake devs and this is a necessary step now.* Comment on "Inundated with fake candidates" Reddit post. Reddit [https://www.reddit.com/r/recruiting/comments/1bffeiu/inundated_with_fake_candidates/?rdt=34969]
- BeFunky (2025) *AI Image Enhancement*, Retrieved from [https://www.befunky.com/features/portrait-enhancer/] on February 27, 2025
- Froehlich A. (2024, May 4) *How to detect deepfakes manually and using AI,* Retrieved from [https://www.techtarget.com/searchsecurity/tip/How-to-detect-deepfakes-manually-and-using-AI] on February 27, 2025
- Strong_Ad_4 (2024) *What I adore are people who say their name is Gabriel Figueroa but they have such a thick Asian accent they cannot pronounce it. I also had a guy tell me he enjoyed his view of the Pacific from his balcony in Miami.* Comment on "Inundated with fake candidates" Reddit post. Reddit [https://www.reddit.com/r/recruiting/comments/1bffeiu/inundated_with_fake_candidates/?rdt=34969]
- Bake-Capable (2024) *[...] I feel like I'm going crazy because just about every application is a fraud when doing a little digging. I even had one LI application where the profile pic was a stock picture from Walmart ad (...). Inundated with fake candidates" Reddit post. Reddit [https://www.reddit.com/r/recruiting/comments/1bffeiu/inundated_with_fake_candidates/?rdt=34969]*
- HR Research & HR.com (2021) *How often employers conduct background checks based on type of employment.* [https://pubs.thepbsa.org/pub.cfm?id=FB36B937-C9D5-A941-7720-4047386F38B0]