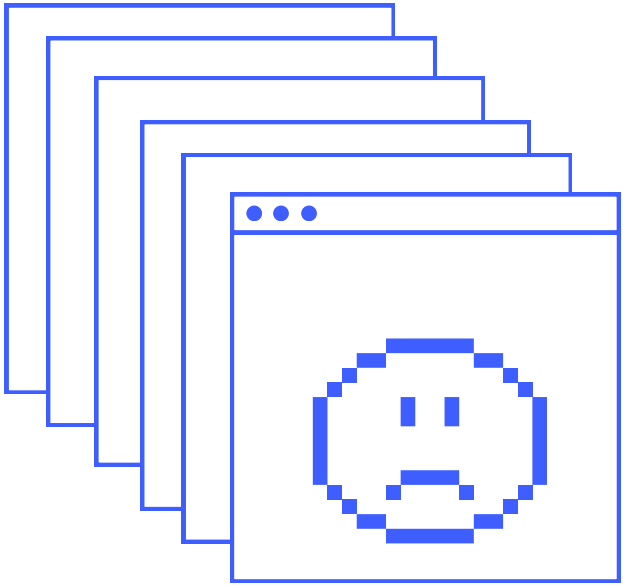
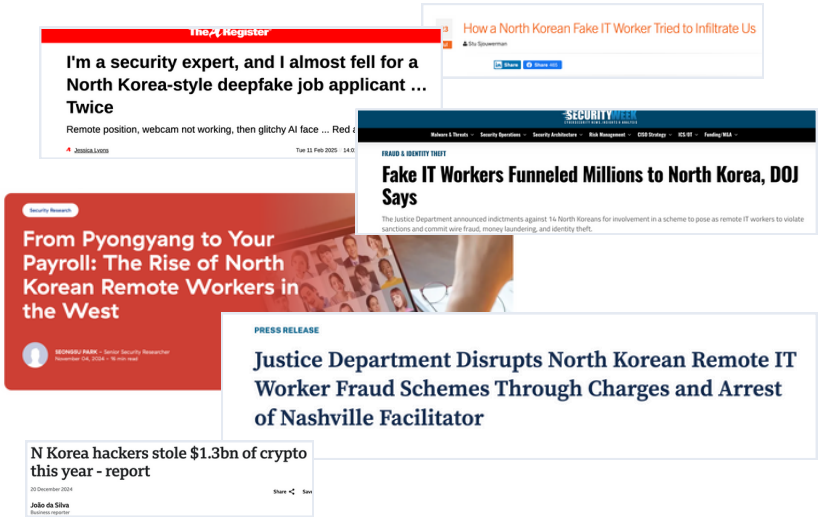
Deepfake Fraud Prevention

17 Practical Strategies to Detect Fake IT Workers



VIDOC
Security lab

Global Threats



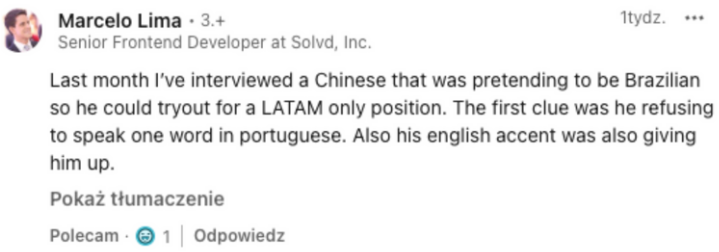
The rise of fake remote workers using AI [1]

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's comment under our viral AI developer video on LinkedIn, [LINK], online: February 17, 2025

In 2024, the U.S. Justice Department took down a North Korean fraud scheme involving remote IT jobs *("Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator", [LINK], online: February 27, 2025)*.

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's comment under our viral AI developer video on LinkedIn, [LINK], online: February 17, 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.

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 Operations in Vidoc Security Lab*

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 Operations in Vidoc Security Lab*

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.

Want to Know More?

If you found this excerpt useful and want to deepen your understanding of how to identify fake candidates, **we invite you to explore our full free ebook.** It's packed with practical insights, real-world examples, and expert tips to help you stay ahead of evolving threats in the hiring process.

But that's not all—if you're interested in sharing this knowledge with your team, **we've also prepared a dedicated presentation that expands on these topics.** This presentation is designed to help hiring managers, recruiters, and security teams better recognize and prevent fraud in the recruitment process. Feel free to reach out!

You can access the complete ebook for free on our website: vidocsecurity.com/ebook.