# Hiring Remote IT Workers? Beware the Deepfake Frauds

Hundreds of U.S. firms have been infiltrated by foreign nationals posing as American citizens. And now with new open-source tools, it's easier than ever to create deepfake videos of job applicants. Here's how to sharpen your hiring process.

Perspective

**OCTOBER 31, 2024**

After an exhaustive search, the hiring managers at KnowBe4 thought they had identified the ideal candidate to join the company's internal AI team.

On paper, Kyle ticked all the right boxes for the developer position. He was an experienced software engineer, presented well in all of his video interviews, and had excellent references. His background credentials checked out.

But after the security firm shipped Kyle his company laptop, weird things started to happen. First, he tried installing malware on the machine, and it was halted by the system's endpoint protection software. When the company's security operations center reached out over Slack, Kyle claimed he'd accidentally compromised his system while troubleshooting his router.



That excuse made no sense, so the security team tried to get him to join an audio chat. Kyle said he couldn't talk and then stopped communicating entirely. That was enough

**Dan Tynan**

Dan Tynan is an award-winning journalist whose work has appeared in *Adweek, Fast Company, The Guardian, Wired,* and too many other publications to mention.

## Key takeaways

- Thousands of North Korean nationals pretending to be American citizens have been hired by U.S. companies
- As AI deepfakes proliferate, fake employees will be increasingly difficult for HR departments to identify.
- Infiltrated companies are more at risk for data breaches, financial fraud and supply chain attacks.

for the SOC [security operations center]. Within less than 30 minutes, KnowBe4 had locked down Kyle's account. It then shared the details of their exchanges with security consultancy Mandiant and, later, the FBI.

"Between Mandiant and the FBI, we learned that this was a sophisticated, well-funded, state-sponsored operation," says Stu Sjouwerman, the firm's CEO, who blogged about the incident in July as part of an effort to warn other companies.

Though for hundreds of U.S. companies, and even more around the globe, that warning comes too late.

**300+**

**companies have been infiltrated by North Korean IT workers pretending to be U.S. citizens**

## We need to talk about Kyle...and deepfakes

As a leader in innovative security awareness training, KnowBe4 is no stranger to threat intelligence trends and smart cyber hygiene. Which only underscores how insidious the Kyle problem is. They learned that "Kyle" was most likely a North Korean national pretending to be an American citizen. To evade the company's employee screens, he had used a stolen identity and an AI-doctored photo to pass background checks. A professional shill was paid to play Kyle in the video interviews, while the actual employee was probably somewhere in Asia. References were confirmed via email.

supply chain attacks.

### Focal Point

Dedicated to helping business executives and IT leaders effectively use technology to connect with customers, empower employees and achieve better results.


Technology & Innovation Reporting - National
Government Coverage - Pacific Region
Technology & Innovation Reporting - Pacific Region

### Tanium Subscription Center

Get Tanium digests straight to your inbox, including the latest thought

> **With a single high-resolution image of someone's face and about 10 seconds of audio, you can use an open-source tool to fool anybody on Zoom or Teams.**
>
> Ben Colman, CEO and co-founder, Reality Defender

Sjouwerman emphasizes that no company data was lost, no sensitive systems were breached, and KnowBe4's security defenses worked exactly as they were supposed to. Kyle was immediately dismissed.

Still, Sjouwerman admits his company dodged a bullet. If the faux developer hadn't immediately tried to install malware, he might have gained access to the company's software repositories and cloud servers.

[Read also: "Deepfake" wasn't even a word a few years ago – test your knowledge of AI vocabulary here]

Sjouwerman's admission is rare, but the attack his company suffered is not. Shortly after he posted his account, KnowBe4 heard from more than a dozen other companies that had received applications from similar fake candidates, one of whom had even hired "Kyle."

## Attackers are hiding in plain sight

According to the U.S. Department of Justice, more than 300 companies have been infiltrated by North Korean IT workers pretending to be U.S. citizens. This includes both Fortune 500 firms and organizations with as few as 12 employees, notes Roger Grimes, a data-driven defense evangelist for KnowBe4, and author of a white paper detailing how to identify and prevent similar attacks.

As of May 2024, fraudulent foreign-based employees had collected nearly $7 million in salary from U.S. firms. According to the FBI, most of that money was funneled directly to the North Korean government to help fund its weapons programs.

**$7M**

**Salary collected from U.S. firms by fraudulent, foreign-based employees**

These foreign IT workers were aided by a network of stateside "facilitators." These collaborators operate laptop farms that are discreetly accessed by employees located overseas, as well as provide false references, money laundering, and other services. Last May, the DOJ arrested two Americans for their role in helping foreign IT workers

dupe their U.S. employers.

In most cases – and here's the kicker worth underscoring for enterprise leaders – the foreign employees *appear to have performed the work they were hired to do.* These are not slackers, and so not that easy to spot. Of course, unwittingly employing IT workers from the Democratic People's Republic of Korea (DPRK) opens up any organization to an array of risks.

[Read also: As layoffs at various workplaces continue, the risk rises of insider threats – here's how to spot them]

Hiring anyone from North Korea may violate **international sanctions** against that country, potentially putting companies in legal jeopardy. Having an employee from a hostile nation-state also means the company is more likely to face **insider attacks**, notes Sjouwerman. North Korean universities produce a lot of IT workers and black hat hackers, he says, and they all know each other. Companies that have been infiltrated are more vulnerable to **data breaches**, **financial fraud**, and **supply chain attacks**.

"Just imagine if the black hat sends a text to his IT pal at Morgan Stanley: 'Hey, someone at Morgan Stanley is saying bad things about Kim Jong-Un. Wreak as much damage as you can.'"

## Deepfakes are getting deeper and easier

In retrospect, there were a few red flags KnowBe4 should have recognized, Sjouwerman admits.

> **There are thousands of these people around the world working for companies that have no clue.**
>
> Stu Sjouwerman, CEO, KnowBe4

For example, while “Kyle” claimed to live in Atlanta, he asked KnowBe4 to send his company laptop to an address in Washington state – the location of one of the known laptop farms. Sjouwerman adds that his team should have been more thorough in looking for discrepancies in the applicant’s work history and vetting his references. Since then, the company has significantly revamped its hiring processes.

But because these are sophisticated, **state-run operations**, they may have already switched up their tactics, warns Grimes.

In addition, the growing sophistication of AI deepfake videos will make doing remote job interviews even more precarious, notes Ben Colman, CEO and co-founder of Reality Defender, which offers deepfake detection services to enterprises.

[Read also: Fight AI with AI – here's your ultimate guide to AI cybersecurity]

Over the past 18 months, the cost of creating deepfakes has dropped 100 times, notes Colman. Coupled with an explosion of open-source face- and voice-mapping tools, it is easier than ever to create believable real-time videos of virtually anyone, saying virtually anything, which will only fuel an onslaught of **misinformation** and **disinformation**.

"With a single high-resolution image of someone's face and about 10 seconds of audio, you can use an open-source tool to fool anybody on Zoom or Teams," he adds.

Colman says Reality Defender is working with HR and recruiting teams at large banks, media, and government agencies as part of their employee verification process. But for the most part, broad awareness of the faux remote-worker problem is lacking.

“There are thousands of these people around the world working for companies that have no clue,” says Sjouwerman. “I would strongly recommend other CEOs assess their existing hiring practices, and in particular sharpen up the process of hiring remote engineers.”

[Listen also: Why your next big hire should be a chief AI officer, but be warned – you can’t trust half of those you find on LinkedIn]

Companies need to **threat model** their recruitment processes and inform senior management of the risks of hiring foreign nationals, Grimes says. During interviews, ask questions that someone who graduated from a particular university, lived in a specific city, or worked at a previous employer would be likely to know but whose answers aren’t easily found online.

When possible, the surest way to vet someone is in person, he adds.

“If possible, always require that remote employees physically meet with an employee, team leader, or selected agent of the organization in person, with an official ID, to confirm they are who they say they are.”

## 10 telltale signs that your IT job candidate might not be legit:

**While there's no 100 percent surefire way to detect a fake applicant, the following warning signs should prompt any hiring manager to dig a little deeper.**

- **1. Lack of English proficiency** despite claims of U.S. education or longtime residency
- **2. Accent doesn't match** region of world they claim to be from
- **3. Answers to work history questions** are inconsistent or vague
- **4. Minimal digital footprint** outside of supplied profiles
- **5. Inconsistent or newly created** social media identities
- **6. Job descriptions or work product copied** from other sources
- **7. Only uses public email domains** like Gmail or Outlook.com
- **8. Always connects** via VPN or VoIP numbers
- **9. Phone interviews** conducted from noisy call centers
- **10. Hesitant to appear on camera**, makes excuses as to why

## Related

What Return-to-Office (RTO) Means for Your Cybersecurity

I Almost Fell for This Online Scam. Why Even Tech Pros Can Be Taken

How AI Is Redefining Data Loss Prevention (DLP)