How AI services power the DPRK's IT contracting scams

By Okta Threat Intelligence

Published: 2025-04-24 · Archived: 2026-04-05 14:00:41 UTC

Over the past few months, Okta Threat Intelligence conducted in-depth research into online services used by individuals identified by US authorities and trusted third parties as agents for the Democratic People's Republic of Korea (DPRK).

Our research finds that generative artificial intelligence (GenAI) is playing an integral role in how North Korean nationals gain employment in remote technical roles around the globe, in what some researchers refer to as "DPRK IT Workers" or "Wagemole" campaigns. GenAI is used to create compelling personas at numerous stages of the job application and interview process. Once employed, GenAI tools are also used to assist in maintaining multiple simultaneous roles to earn revenue for the state.

Okta Threat Intelligence has observed multiple AI-enhanced services used to:

- Manage the communications of multiple personas and their numerous mobile phone accounts, instant messaging accounts, email accounts and other related chat services behind a "single pane of glass"
- Translate, transcribe and summarize communications
- Generate and critique CVs and cover letters
- Conduct mock job interviews via chat and webcam
- Test and improve the likelihood of any given job application passing automated checks

Okta Threat Intelligence has also observed facilitator use of online shipping and logistics services. We hypothesise that these services are used to redirect company-issued devices to "laptop farms" operated by facilitators based in Western countries.

Background

Multiple arrests and indictments have revealed the scale at which individuals operating on behalf of the DPRK have been mobilized into neighbouring countries to gain fraudulent employment in organizations across the globe.

The primary objective of these schemes is to raise funds for the DPRK and compensate for the significant financial sanctions applied to the North Korean regime. US agencies have also identified several outlier cases in which the access to systems provided for employment was used to facilitate espionage or data extortion.

The targets for these fraudulent schemes appear opportunistic and based on the availability of remote technical roles. The employers most at-risk are technology companies that are more likely to accept remote candidates for

IT or software engineering roles, often on a contingent basis. However, these campaigns also extend to industry verticals well beyond the technology sector.

Okta Threat Intelligence has worked with highly targeted customers and partners, with a view to developing preventative controls for this unique threat model. In the process, Okta has revised our own onboarding processes, shared awareness collateral and built out numerous methods of detection.

The research had a direct influence on feature enhancements built into Okta Workforce Identity, such as ID verification services, that Okta customers can use to reduce their exposure to this threat.

The Facilitators

Our understanding of this threat is shaped by the unique insight Okta Threat Intelligence can glean into the tools used by those individuals identified as “facilitators” of fraudulent employment schemes.

These facilitators provide the necessary in-country support, technical infrastructure and/or legitimate business cover to help individuals from sanctioned countries gain and maintain employment.

Facilitators already apprehended by law enforcement in the United States are alleged to have knowingly provided a range of support services to DPRK nationals:

- Direct assistance in the recruitment process
- A domestic address for the shipment of company-issued devices
- Access to legitimate identity documents
- Operating company-issued devices on the remote worker’s behalf
- Installing remote management and monitoring (RMM) tools on the device to facilitate the remote work
- Authenticating, where necessary, on the remote worker’s behalf

One Arizona-based “laptop farm” operation exposed in May 2024 is alleged to have assisted in the placement of over 300 individuals in technical positions across the United States. In another January 2025 indictment, two US residents were accused of fraudulently obtaining employment and operating a laptop farm in North Carolina for DPRK nationals, after they’d successfully gained employment at 64 organizations.

Okta can now reveal for the first time the degree to which facilitators of fraudulent work schemes rely on emerging GenAI-enhanced services to scale their operations.

Okta customers can read a comprehensive report into DPRK IT Worker fraud at the Okta Security Trust Center. Primary Security Contacts can sign-in to access threat advisories at **security.okta.com**

In recent months, individuals strongly suspected to be DPRK-created personas have been recorded using real-time “deepfake” video during interviews.

Okta Threat Intelligence research has observed a far broader set of GenAI services used in these schemes, suggesting a very deliberate attempt by facilitators to keep pace with AI innovation. Facilitators are now using GenAI-based tools to optimize every step in the process of applying and interviewing for roles and to aid DPRK nationals attempting to maintain this employment.

Facilitators were observed using GenAI-based services specializing in:

- Unified messaging
- Recruitment platforms
- Resume/CV screening
- Candidate management
- Automated job screening
- AI-based chatbots
- AI code training
- Online shipping

While Okta Threat Intelligence is not able to observe the facilitators' activities beyond the login page, the narrow range of functionality offered by many of these tools allows us to hypothesize on some likely use cases:

1. Unified messaging

One of the most demanding challenges for facilitators is how to manage multi-channel communications on behalf of dozens of candidates from sanctioned countries and their multiple personas.

Okta Threat Intelligence observed the use of unified messaging services to manage many simultaneous mobile phone accounts, instant messaging accounts, email accounts and other related chat services behind a "single pane of glass". These GenAI-enhanced services are required to manage the scheduling of job interviews with multiple DPRK candidate personas by a small cadre of facilitators.

These services use GenAI in everything from tools that transcribe or summarize conversations, to real-time translation of voice and text.

2. Recruitment platforms

Facilitators and candidates both make extensive use of jobseeking platforms to apply for roles.

More surprising was the use of AI-enhanced recruitment platforms typically used by recruiters (not candidates) to amplify the reach and accuracy of job postings.

Access to these tools provides facilitators opportunities to advertise roles at front companies that are similar, if not identical, to those advertised by targeted organizations, in order to study the cover letters and resumes of

legitimate candidates. The CVs and cover letters from legitimate jobseekers may even form part of a training set for optimizing future applications made on behalf of DPRK nationals.

These same recruitment platforms provide access to the same applicant vetting systems (ATS) real employers use to narrow down the number of job applications a recruiter or hiring manager needs to manually review. Posting fake job advertisements would allow facilitators to examine what features presented in a job application are most likely to result in these AI-enhanced algorithms selecting a particular candidate over others.

At scale, these techniques dramatically improve the potential success of job applications, effectively using the recruiters own tools against them at scale.

3. Resume/CV screening

Okta Threat Intelligence assesses that facilitators are highly motivated to generate successful cover letters, CVs and interviews and address any specific criteria in a given application. Facilitators were observed making use of services that provide “AI Superpowers” to job applicants to help them “outsmart employers’ robots”, in order to improve the chances of a job application successfully progressing past the automated CV/resume scans used in recruiting platforms.

These services use GenAI agents to test uploaded CVs against ATS (applicant tracking software), iterating until they achieve a better result and learning which personas will be more successful in any given role.

4. Candidate management

Okta Threat Intelligence observed services that use GenAI agents to automate the process of filling in application forms on behalf of candidates and to track the progress of candidates through the application process.

Again, these capabilities address the challenge of facilitating job applications and employment on behalf of multiple individuals and their multiple personas over multiple timezones.

5. Mock interviews

Once an application is successful, the next task for facilitators is to prepare their candidates (or the facilitator themselves, in some cases) for job interviews.

Facilitators were observed using AI-enhanced services that deploy GenAI agents to host and record first-round interviews on behalf of employers, then critique and offer improvement tips for the interviewee.

These automated “AI-based webcam interview review” services claim to assist with the appropriate use of lighting, video filters, lighting and the candidate’s approach to conversation.

Okta Threat Intelligence assesses that mock interviews staged by AI agents can be used to evaluate the efficacy of deepfake overlays and of highly scripted answers to common questions, to decrease the chance of their ruse being discovered.

6. LLM-based chatbots

While most of the GenAI applications used by facilitators relate directly to training and recruitment, Okta Threat Intelligence also observed them constantly signing into generic chatbots powered by large language models (LLMs).

Analyzing patterns of activity, these GenAI tools appear to be relied on heavily throughout the recruitment process, as well as by successful candidates once they gain employment.

7. Code training services

Candidates were also observed signing into free services that offer training in specific development languages and AI tools. These training platforms deliver a cursory awareness of unfamiliar development skills required by a hiring organization at interview, and the bare essentials required to maintain employment for as long as possible.

In short, DPRK facilitators are AI's "power users"

By extensively employing AI-enhanced tools, facilitators enable minimally skilled, non-native English-speaking workers to maintain software engineering positions long enough to channel earnings towards the sanctioned DPRK regime.

The scale of observed operations suggests that even short-term employment for a few weeks or months at a time can, when scaled with automation and GenAI , present a viable economic opportunity for the DPRK.

Mitigating Controls

To mitigate the threat posed by these campaigns, Okta Threat Intelligence recommends:

- Embedding Identity Verification in key business processes,
- Training staff to identify common indicators of fraudulent behavior
- Detecting the unauthorized use of RMM (remote management and monitoring) tools

Okta customers can access a detailed set of recommendations and detection methods by selecting **Okta Threat Intelligence** at **security.okta.com.**

Liam Dermody, Tim Peel, Alex Tilley and David Zielezna contributed to this research.
