# North Korean hackers use AI to secure and exploit remote jobs in western firms



New research from cybersecurity firm Okta has revealed that North Korean hackers are employing generative artificial intelligence (GenAI) technology to secure and maintain remote employment in western companies, particularly in sectors with sensitive security data such as defence, aerospace, and engineering. This development marks an escalation in an ongoing campaign where hackers seek to infiltrate firms through fake job applications and interviews.

According to Okta’s findings, the Democratic People’s Republic of Korea (DPRK) actors are leveraging AI to create convincing personas at various stages of the job application and interview process. This includes generating comprehensive CVs and cover letters crafted by AI models, conducting mock interviews via chat and webcam, and handling communications through translation and summarisation tools. The use of GenAI enables these hackers to juggle multiple remote job roles simultaneously, thereby generating significant revenue for the DPRK state.

The campaign is supported by a network of facilitators within North Korea who provide critical in-country assistance. These facilitators supply technical infrastructure, legitimate business covers, domestic addresses, and authentic documentation to help the hackers present credible profiles throughout recruitment and hiring processes.

In a further development of their tactics, North Korean hackers are also reversing their approach by using fake interviews to target job seekers. In such scenarios, malware and information-stealing software are deployed through the interview process. The attacks often start on established professional platforms such as LinkedIn and Upwork, where the attackers initiate contact to discuss supposed job opportunities.

The growing sophistication of these schemes highlights the complex and multi-faceted nature of the threat, demonstrating how AI technologies are being weaponised in cyber-espionage efforts connected to employment fraud.

The Tech Radar report advises vigilance among job seekers and employers alike, urging scrutiny of communications during hiring processes and caution before downloading any unfamiliar software. The evolving use of AI in such campaigns represents a significant shift in cyberattack methods targeting critical industries in the West.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://sec.okta.com/articles/2025/04/GenAIDPRK/> - This article from Okta Threat Intelligence details how North Korean hackers are using generative artificial intelligence (GenAI) to secure remote employment in Western companies. It explains the use of AI-generated CVs, cover letters, mock interviews, and communication management tools enabling hackers to maintain multiple remote roles for revenue generation, corroborating the primary claims about the hacking campaign and AI usage.
2. <https://www.techradar.com/pro/security/north-korean-hackers-are-using-advanced-ai-tools-to-help-them-get-hired-at-western-firms> - The Tech Radar article confirms that North Korean hackers are leveraging advanced AI tools in their fake job application and interview campaigns targeting sectors with sensitive data like defense and aerospace. It also highlights how AI is used to create convincing personas and maintain multiple job roles, matching the description of the campaign’s sophistication and scale.
3. <https://cybersecuritynews.com/north-korean-hackers-using-genai/> - This Cybersecurity News report expands on North Korea’s use of GenAI and the role of facilitators in the West providing infrastructure and managing devices for the hackers. It details the financial motivation behind the scheme and the use of deepfake video technology in interviews, supporting the article’s points about facilitators, technical infrastructure, and advanced deception methods.
4. <https://thehackernews.com/2025/04/north-korean-hackers-spread-malware-via.html> - The Hacker News article discusses how North Korean hackers also employ fake interviews as a vector for spreading malware and stealing information from job seekers, starting their attacks through platforms like LinkedIn and Upwork. This corroborates the article’s claim about the reverse use of fake interviews to target job seekers with malware.
5. <https://gbhackers.com/north-korean-hackers-exploit-genai/> - GbHackers provides an overview of how DPRK-linked operatives utilize GenAI to gain remote jobs worldwide. It discusses the AI-driven persona creation and the use of facilitators to maintain credibility during recruitment, supporting the article's points about the multi-faceted nature of the threat and the use of legitimate business covers.
6. <https://www.noahwire.com> - This is the original source attributed for the summarized article, providing comprehensive coverage of the North Korean hackers’ campaign using generative AI to infiltrate Western companies, and advising caution for job seekers and employers, aligning with the article’s final advice on vigilance in the hiring process.
7. <https://www.techradar.com/pro/security/north-korean-hackers-are-using-advanced-ai-tools-to-help-them-get-hired-at-western-firms> - Please view link - unable to able to access data