KIBU

Quarterly Threat Report

Q1 2026

IS YOUR COMPANY INADVERTENTLY FUNDING NORTH KOREA'S WMD PROGRAM?

This threat report launches our quarterly series examining emerging cybersecurity issues. Each report analyzes contemporary cyber threats through real-world examples and case studies, then provides actionable solutions for security teams.

North Korean state-sponsored threat actors have weaponized social engineering, particularly phishing attacks, to create a growing "fake employee" problem. These operatives secure legitimate positions at companies worldwide, funneling their salaries back to the DPRK regime. Recent campaigns demonstrate an urgent need for reliable identity verification before the hiring process begins. This report examines how falsified identities backed by stolen or fabricated credentials are penetrating organizations, and explores verification tools that can prevent these single points of failure.

The New Threat

KIBU

Social engineering scams such as phishing attacks, have fueled the “fake employee” problem emanating from threat actors sponsored by North Korea. Numerous cyber campaigns and incidents highlight the increasing need for reliable, human verification online. This report outlines the evolving threat around falsified human identities supported by valid credentials in digital systems, and calls for novel approaches to prevent single-points-of-failure that lead to compromise.

The Evolution of Social Engineering

In the past, the most dangerous online threats were technical vulnerabilities like zero-day exploits and man-in-the-middle (MITM) attacks. Today, the most prevalent threats target the weakest link in digital security: legacy credentials. These authentication systems create opportunities for human error: hanging credentials (like an open SharePoint link), exposed credentials (such as weak passwords), or stolen credentials (through SIM swapping attacks).

Social engineering scams date back to the internet's earliest days. The infamous "Nigerian Prince" email promised substantial windfalls in exchange for a small upfront "transaction fee[1].” As these techniques entered the public consciousness, such obvious phishing attempts became easy to recognize. Often, the absurdity was intentional: outlandish claims filtered out skeptics, ensuring scammers only engaged the most susceptible targets and maximized their conversion rates.

Over time, social engineering has grown dramatically more sophisticated. AI tools now enable threat actors to scale both the volume and quality of attacks at minimal marginal cost, flooding the top of their "fraud funnel." The result: social engineering has become alarmingly effective. One estimate suggests that in 2024, 98% of successful cyber intrusions began with a social engineering attempt[2]. Now, with AI agents masquerading as legitimate humans, the asymmetry increasingly favors attackers over defenders.

The AI Amplification Effect

Generative AI possesses unprecedented capabilities to learn from and replicate human behavior. Historical scams created an expectation that attacks would be recognizable and stoppable before causing serious damage. Even experienced security professionals anticipate obvious red flags, making sophisticated scams that leverage genuine personal or corporate details nearly undetectable. Operations that just two years ago required numerous human accomplices, sometimes enslaved workers[3], can now be executed using low-cost large language models.

In 2024, scams surpassed digital payment fraud to become the leading fraud category, with financial losses rising 121%[4]. Unlike payment fraud, which involves unauthorized use of funds, scams manipulate victims into willingly surrendering information or capital. The objectives extend beyond intercepting payments to stealing intellectual property, customer data, personally identifiable information (PII), or establishing footholds for ransomware attacks.

A recent survey of 3,000 IT and cybersecurity professionals in the 2026 ISACA Tech Trends and Priorities report ranked AI-driven social engineering attacks as the top cyber threat for 2026[5]. Any threat actor can now launch these attacks—the only constraint is how convincing the scheme appears to a single vulnerable network user.

When Hostile Actors Exploit the Gap

What happens when sophisticated adversaries weaponize these manipulative techniques? What happens when falsified identities bypass zero trust frameworks, network analysis, and encryption by simply obtaining valid credentials?

The consequences are staggering: threat actors can circumvent U.S. and U.N. sanctions, secure employment in foreign markets, and directly fund authoritarian regimes and WMD programs.

1. Akeiber, Hussein Jassim. “The evolution of Social Engineering Attacks: A Cybersecurity Engineering Perspective.” Al Rafidain Journal of Engineering Sciences, vol. 3, no. 1, 18 Feb. 2025, pp. 294–316, https://doi.org/10.61268/r9c49865.
2. Kidd, Chrissy, and Muhammad Raza. “What Are Social Engineering Attacks? A Detailed Explanation.” Splunk, 6 Aug. 2024, www.splunk.com/en_us/blog/learn/social-engineering-attacks.html#:~:text=98%25%20of%20cyberattacks%20rely%20on,engineering%20attack%20is%20around%20$130%2C000.
3. Wong, Tessa, et al. “Cambodia Scams: Lured and Trapped into Slavery in South East Asia.” BBC News, BBC, 20 Sept. 2022, www.bbc.com/news/world-asia-62792875.
4. “Scam-Related Fraud Jumped 56% in 2024, Surpassing Digital Payment Crimes.” PYMNTS.Com, 10 Dec. 2024, www.pymnts.com/news/security-and-risk/2024/scam-related-fraud-jumped-56percent-surpassing-digital-payment-crimes/.
5. Poireault, Kevin. “AI Social Engineering Top Cyber Threat for 2026, Isaca Survey Reveals.” Infosecurity Magazine, Infosecurity Magazine, 20 Oct. 2025, www.infosecurity-magazine.com/news/ai-social-engineering-top-cyber/.

DPRK Fake Employees

KIBU

Identity is the Weakest Link

While North Korea has long leveraged its cyber capabilities to support state-sponsored espionage, disinformation, and sabotage initiatives[6], they have more recently added a critical dimension: generating hard currency to counteract economic collapse and international sanctions.

Initially, observers assumed these schemes funded the regime's elite lifestyles or offset deficits in North Korea's massive conventional military. However, U.S. intelligence has revealed a more alarming reality: one primary motivation behind DPRK-sponsored cybercrime is raising funds specifically for advanced weapons development.

High-Profile Attacks: A Patter of Escalation

Several notorious incidents illustrate the DPRK's cyber capabilities:

- 2014: Sony Pictures attack – An attempt to prevent the release of The Interview, a satirical film targeting North Korean leadership
- 2016: Bangladesh Bank heist – Theft of $81 million USD designed to generate hard currency
- 2017: WannaCry outbreak – Global ransomware attack that crippled organizations worldwide[7]

These incidents didn't occur in isolation. The DPRK has conducted a multi-decade campaign against a broad range of Western targets. Astonishingly, it's estimated that illegal cyber attacks now provide 40% of the DPRK's WMD funding[8]. Their methodology has consistently adapted to prevailing cybercrime trends. They deployed WannaCry when zero-day exploits dominated, and now they are capitalizing on social engineering via generative AI as organizations struggle to address this emerging threat.

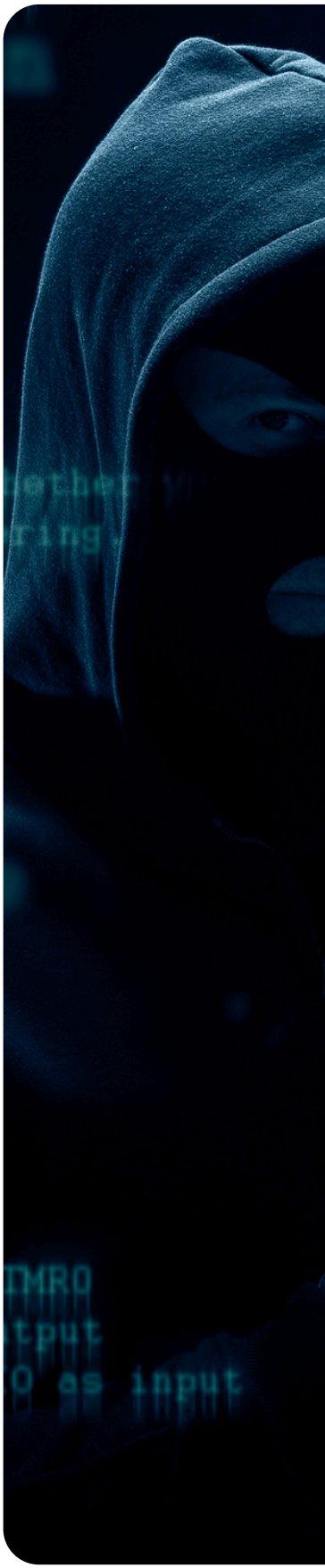
The Shift to Identity-Based Attacks

As enterprises spent the past decade deploying zero-trust frameworks (including multi-factor authentication) and completing cloud migrations that strengthened network-level defenses, the DPRK adapted by finding remaining vulnerabilities. They discovered a critical weakness: identity verification. Why bother stealing credentials or breaking encryption when you can simply create fake employees who are handed valid credentials? Welcome to the era of the "fake human."

The “Jasper Sleet” Program: How the Scheme Works

The DPRK's current campaign, often called "Jasper Sleet," follows a straightforward playbook:

- **Fabricate identities** – IT workers in North Korea and China create false personas complete with fake names, faces, identification documents, and even synthesized voices
- **Flood job markets** – They submit applications en masse, particularly targeting IT companies and remote positions
- **Secure employment** – Eventually, these fabricated identities obtain positions at Western companies
- **Maintain the illusion** – They use generative AI to complete work tasks and appear as legitimate employees
- **Expand access** – They gain additional responsibilities and move laterally within organizations
- **Exfiltrate and monetize** – They steal data for sale or leverage, funneling paycheck revenue to fund government activities, including WMD development



6. Tidy, Joe. “North Korean Hackers Stealing Record Sums, Researchers Say.” BBC News, BBC, 7 Oct. 2025, www.bbc.com/news/articles/cwy8z7wxe03o.
7. “North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.” Department of Justice, 6 Feb. 2025, www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
8. Seshadri, Chandana. “How DPRK IT workers exploit identity management vulnerabilities.” The RUSI Journal, vol. 170, no. 4, 7 June 2025, pp. 74–84, https://doi.org/10.1080/03071847.2025.2532012.

The Scope of the Threat

For U.S. CISOs, this represents an almost incomprehensible reality: your organization is being defrauded, your intellectual property stolen to advantage (often hostile) competitors, and the money diverted to build biological, chemical, and nuclear weapons that may one day threaten American citizens.

The financial scale is staggering:

- Individual DPRK IT workers have earned over $300,000 USD annually
- A December 2024 Department of Justice indictment revealed that just 14 DPRK nationals generated over $88 million USD over six years in the United States[9]
- Some estimates suggest North Korean cybercrime has secured over $2 billion USD for the regime[10]

These nationals worked for DPRK-controlled companies in China and Russia, using borrowed, stolen, or fabricated identities to mask their North Korean origins. They obtained remote IT employment at U.S. firms, sometimes collaborating with U.S. citizens to install company-issued laptops with remote access software—making the scheme more convincing by circumventing certain network detection methods[11].

Global Reach and Operational Sophistication

While the majority of these operatives work from China, they've been identified in the United States, Germany, Portugal, the UK, Australia, and Japan, often in sectors including AI, web development, and even positions with government agencies or contractors[12].

The threat extends beyond wage theft. Operatives have:

- Stolen company data and demanded ransom payments[13].
- Implanted vulnerabilities for future exploitation
- Targeted Fortune 500 companies (SentinelOne alone received over 1,000 DPRK-linked job applications)[14]
- Used AI to work 10+ jobs simultaneously by automating task completion[15]

Key Takeaways:

1. **AI-powered social engineering now drives 98% of successful cyber intrusions**, with scam losses up 121% in 2024 as attackers scale sophisticated operations at minimal cost.

2. **North Korean "fake employees" use fabricated identities to secure legitimate remote IT jobs**, bypassing security by receiving valid credentials rather than stealing them.

3. **These operations have generated an estimated $2 billion for the DPRK regime**, funding approximately 40% of their WMD programs while stealing intellectual property.

4. **Identity verification at hiring is the critical security gap** that organizations must address as traditional network defenses prove insufficient against credentialed insiders.

9. “Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions.” Department of Justice, 12 Dec. 2024, https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information.
10. McManus, Michael. “The World’s Poorest Cyber Giant: North Korea’s Multi-Billion-Dollar Hacking Empire - Henry Jackson Society.” Henry Jackson Society, 10 Oct. 2025, henryjacksonsociety.org/2025/10/10/the-worlds-poorest-cyber-giant-north-koreas-multi-billion-dollar-hacking-empire/.
11. “Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions.” Department of Justice, 12 Dec. 2024, https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information.
12. “The DPRK’s Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities.” Multilateral Sanctions Monitoring Team, 22 Oct. 2025, https://msmt.info/Publications/detail/MSMT%20Report/4221.
13. Sharp, Isaac. “Remote Work Has Opened Australia’s Cyber Backdoor.” The Australian Strategic Policy Institute, 16 Oct. 2025, www.aspistrategist.org.au/remote-work-has-opened-australias-cyber-backdoor/.
14. Miller, Maggie, and Dana Nickel. “Tech Companies Have a Big Remote Worker Problem: North Korean Operatives.” Subscriber.Politicopro.Com, 12 May 2025, www.politico.com/news/2025/05/12/north-korea-remote-workers-us-tech-companies-00340208.
15. Yee, Isaac, et al. “How North Korean It Workers Leverage AI and Vulnerable Americans to Infiltrate US Companies.” CNN, Cable News Network, 5 Aug. 2025, www.cnn.com/interactive/2025/08/05/world/north-korea-it-worker-scheme-vis-intl-hnk/index.html.

Analysis & Implications

KIBU

While “fake employees” operate differently than typical phishing schemes, they exploit similar vulnerabilities in human judgment and organizational processes.

How AI Emplowers Scammers

As technology and AI become increasingly essential to the global economy, demand for IT talent has surged. This creates intense pressure on firms to find, hire, and retain skilled professionals as quickly as possible; a sense of urgency that often sidelines proper security hygiene and rigorous vetting processes.

These fake employees exploit classic social engineering principles:

- **Authority** – While likely not impersonating C-suite executives, their falsified subject matter expertise grants them credibility in their claimed domain[16]
- **Curiosity** – Unique, standout (but fabricated) applications capture HR teams' attention
- **Urgency** – They capitalize on high-stress situations, such as critical hiring needs, to induce lapses in judgment from hiring managers

Humans can identify false profiles given adequate time[17], but external stressors and increasingly sophisticated deception destabilize what would otherwise be effective analysis. This pressure, combined with the growing use of AI in hiring processes[18], makes fake profiles easier to slip through undetected. Spoofed locations, synthetic names, deepfake faces, and AI-generated voices deceive HR officials into extending offers. Once hired, these operatives simultaneously funnel paychecks to the DPRK and exfiltrate data for sale or future leverage.

Why Current Defenses Fail

Existing countermeasures against social engineering have proven inadequate:

- **Security awareness training** – Studies show that priming potential victims with training and warnings does not significantly influence personal information disclosure[19]
- **Multi-factor authentication (MFA)** – While more resilient, MFA can be defeated through MFA fatigue attacks, as demonstrated in the 2022 Uber breach by Lapsus$[20]
- **Resource limitations aren't the issue** – This problem plagues even the largest companies with the greatest capacity to combat threats[21]

Many firms are turning to AI-based solutions:

- **Automated verification** – Using AI to cross-reference selfies with government-issued identification
- **AI detection software** – Attempting to identify synthetic profiles and generated content

However, these AI-powered tools face significant accuracy challenges. Generated texts and profiles frequently bypass detection systems, while genuine submissions are flagged as artificial[22]. This creates a double bind: bad actors slip through while legitimate candidates face unnecessary friction.

The Probability Problem

In this game of probabilities, the current approach is failing on multiple fronts:

- Bad actors continue penetrating defenses
- Qualified candidates are improperly flagged and rejected
- HR departments still succumb to pressure to "fill seats," even when doubts exist about a candidate's authenticity

It's time to fundamentally rethink how we validate hires. Rather than relying solely on technological detection or HR gatekeepers, we need to scale down verification by leveraging trust networks and peer validation, emphasizing approaches that exploit the very human connections that AI agents struggle to replicate convincingly.

16. Miller, Maggie, and Dana Nickel. “Tech Companies Have a Big Remote Worker Problem: North Korean Operatives.” Subscriber.Politicopro.Com, 12 May 2025, www.politico.com/news/2025/05/12/north-korea-remote-workers-us-tech-companies-00340208.
17. Sandy, Christopher, et al. “Can humans detect the authenticity of social media accounts? on the impact of verbal and non-verbal cues on credibility judgements of Twitter profiles.” 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), June 2017, pp. 1–8, https://doi.org/10.1109/cybconf.2017.7985764.
18. Ferrazzi, Keith. “The Ai Recruitment Takeover: Redefining Hiring in the Digital Age.” Forbes, Forbes Magazine, 27 Mar. 2025, www.forbes.com/sites/keithferrazzi/2025/03/27/the-ai-recruitment-takeover-redefining-hiring-in-the-digital-age/.
19. Junger, M., et al. “Priming and warnings are not effective to prevent social engineering attacks.” Computers in Human Behavior, vol. 66, Jan. 2017, pp. 75–87, https://doi.org/10.1016/j.chb.2016.09.012
20. Maude, James. “Lapsus$ Breaches Remind US Service Desks & Insiders often Weakest Link | Beyondtrust.” Beyond Trust, 29 Mar. 2022, www.beyondtrust.com/blog/entry/lapsus-breaches-remind-us-service-desks-insiders-often-weakest-link.
21. Yee, Isaac, et al. “How North Korean It Workers Leverage AI and Vulnerable Americans to Infiltrate US Companies.” CNN, Cable News Network, 5 Aug. 2025, www.cnn.com/interactive/2025/08/05/world/north-korea-it-worker-scheme-vis-intl-hnk/index.html.
22. Halaweh, Mohanad, and Ghaleb El Refae. “Examining the accuracy of AI detection software tools in Education.” 2024 Fifth International Conference on Intelligent Data Science Technologies and Applications (IDSTA), 24 Sept. 2024, pp. 186–190, https://doi.org/10.1109/idsta62194.2024.10747004.

The Kibu Solution

The Trust Deficit in Modern Work

The DPRK fake employee crisis highlights an urgent need: reliable human verification online. A common thread runs through all social engineering threats: a fundamental lack of confidence and trust. Specifically, people cannot confidently verify they're communicating with who they think they're communicating with.

The challenge is formidable:

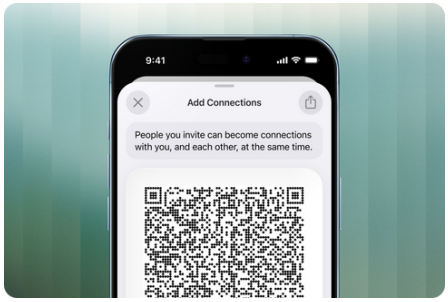
- **AI-powered impersonation** – Chatbots can process thousands of messages in minutes, generating seemingly authentic communications that replicate the patterns of CEOs, coworkers, or job applicants
- **Inadequate existing tools** – Anti-phishing engines struggle with URLs protected by ReCAPTCHA (23)
- **Immature AI detection** – AI detection services remain underdeveloped and prone to false positives

In short, no existing tools provide 100% confidence that digital identities can be trusted.

How Kibu Solves the Problem

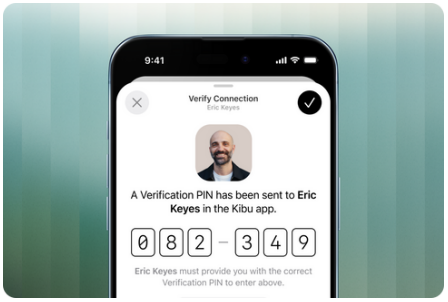
At Kibu, we address this trust gap by ensuring users can verify each other with certainty. When you use Kibu, you form Connections to other users: private, secure channels accessible only to you and your verified Connections from your trusted mobile devices, unlocked with your biometrics. Connections then use the Kibu application to verify each other's identities across video, audio, and text communications. Only your trusted Connection, on their device unlocked with their face, will be able to verify themselves, giving you the confidence that you know who's on the other end of every communication.

HOW IT WORKS



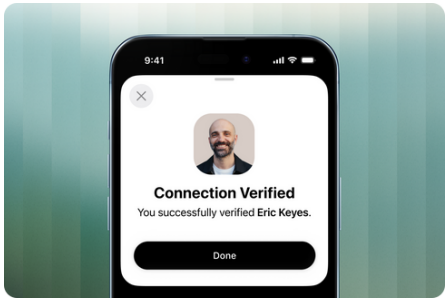
1. Connect

Scan in the Kibu app to instantly add Connections.



2. Verify

Securely verify any Connection's identity via QR code or PIN.



3. Protect

Confidently defend against impersonation-based threats.

About Us

We're bulding the trust layer for the digital world.

Kibu exists because trust should work online the way it works in real life. Real trust flows through human networks. Until now, there was no way to leverage that trust digitally. We believe real-world human relationships can and should defeat digital deception. That small circles of absolute trust can interconnect to build something powerful. That prevention beats detection. That when what's at stake is critical, probability will never be enough.

Learn more at TrustKibu.com →

23. Maroofi, Sourena, et al. "Are you human?" Proceedings of the ACM Internet Measurement Conference, 27 Oct. 2020, pp. 78–86, https://doi.org/10.1145/3419394.3423632.