



| Brief |

Remote IT Workers Fraud: Threats and Prevention

B-2025-04-03a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Fraud, Remote Working, Deepfakes

April 3, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on March 31, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Remote IT Workers Fraud: Threats and Prevention

Key Findings

- Remote IT workers fraud is an emerging threat, with some nation-state actors—such as North Korea—leveraging deepfake-enhanced deception to infiltrate organizations.
- Traditional hiring practices may be insufficient to detect synthetic applicants. Multi-layered identity verification, open source techniques, and biometric checks can help strengthen pre-employment screening.
- Artificial intelligence (AI)-generated profiles and deepfake-assisted interviews have enabled more convincing fraud, highlighting the value of live movement-based identity testing and behavioral screening.
- Post-hire insider threat monitoring may reduce risk, using user activity tracking, biometric analytics, and geolocation validation to identify anomalous behavior.
- Zero Trust security frameworks support risk mitigation by enforcing role-based access control (RBAC) and integrating Data Loss Prevention (DLP) measures.
- Security awareness and insider threat training remain critical components of a resilient workforce, helping employees recognize and report fraud indicators.

| Understanding the Threat: Remote IT Fraud and National Security Risks

Fraud involving remote IT workers has emerged as a notable national security concern, particularly as individuals and groups adopt increasingly sophisticated methods to evade detection. In one recent case, the U.S. Department of Justice (DOJ) disrupted multiple schemes linked to North Korean operatives who used false identities to secure remote IT roles.¹ Salaries from these fraudulent positions were laundered through cryptocurrency networks and used to fund illicit state activities, including cyber operations targeting the financial sector.

A particularly concerning development is the use of deepfake technology to manipulate the hiring process. Fraudulent applicants have been observed using AI-generated facial visuals and voice modifications during interviews to bypass standard identity verification procedures.² In some instances, these individuals have gained access to internal systems and deployed unauthorized software, enabling external actors to exfiltrate sensitive data or disrupt operations.

As remote work becomes more common in IT and technical roles, organizations may need to reassess and strengthen their hiring and security protocols. Traditional resume screening and standard interviews may not be sufficient to detect well-resourced fraud attempts. Integrating advanced vetting tools, behavioral indicators, and insider threat detection mechanisms can help reduce exposure to this evolving risk.

| Pre-Employment Screening: Strengthening Identity Verification and Fraud Detection

A comprehensive pre-employment screening process can serve as an important defense against fraudulent IT applicants. Multi-layered identity verification—such as government-issued ID validation, biometric checks, and open-source research (OSINT)—may help organizations surface inconsistencies in a candidate's work history,

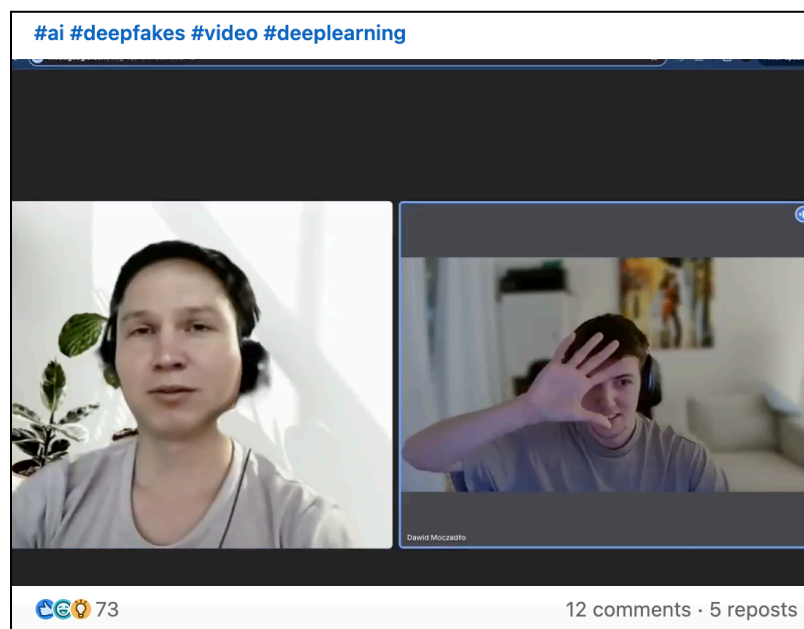
¹

[hXXps://www.justice\[.\]gov/archives/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and](https://www.justice.gov/archives/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and)

² [hXXps://newsletter.pragmaticengineer\[.\]com/p/ai-fakers](https://newsletter.pragmaticengineer[.]com/p/ai-fakers)

credentials, or online presence before the interview stage.³⁴ As synthetic profiles become more prevalent, some companies have adopted additional measures, such as reverse-image searches to identify stolen or AI-generated headshots. These profiles may feature limited social engagement or fabricated professional claims, which can make validation difficult. Where feasible, cross-referencing employment history directly with prior employers—rather than relying solely on references provided by the applicant—may further support legitimacy checks.

The interview process may also require adaptation to counter deepfake-enabled deception. Live video interviews, paired with real-time prompts (e.g., head turns or hand gestures) can help test for visual anomalies that deepfake tools often struggle to replicate dynamically.⁵⁶⁷



Interviewer asks applicant to wave hand to check for signs of AI-generated video during irregular interview footage

Source: LinkedIn

³ [hXXps://www.enisa.europa\[.\]eu/publications/remote-id-proofing-good-practices](https://www.enisa.europa.eu/publications/remote-id-proofing-good-practices)

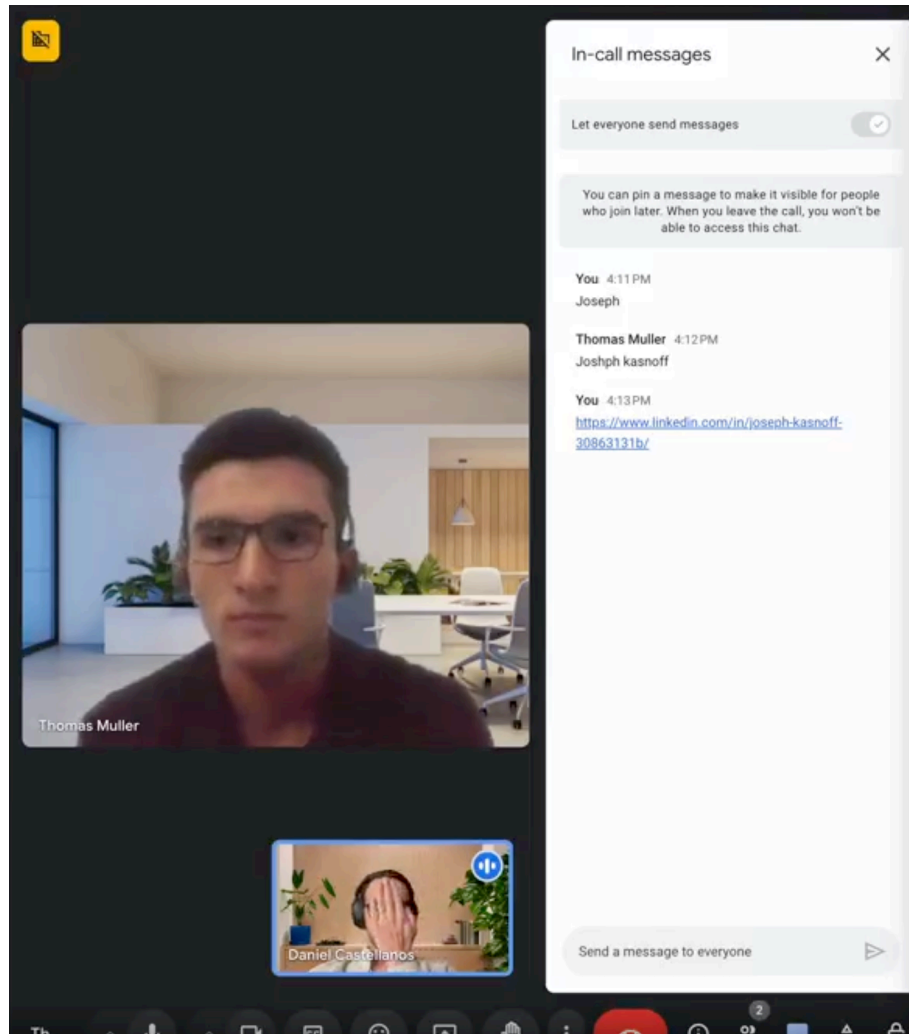
⁴ [hXXps://facetec\[.\]com/2024_ENISA_Remote_ID_Proofing_Best_Practices.pdf](https://facetec[.]com/2024_ENISA_Remote_ID_Proofing_Best_Practices.pdf)

⁵ [hXXps://www.enisa.europa\[.\]eu/publications/remote-id-proofing-good-practices](https://www.enisa.europa[.]eu/publications/remote-id-proofing-good-practices)

⁶ [hXXps://www.linkedin\[.\]com/posts/deividas-mataciunas_ai-deepfakes-video-activity-7306105355246145536-TeDs/](https://www.linkedin[.]com/posts/deividas-mataciunas_ai-deepfakes-video-activity-7306105355246145536-TeDs/)

⁷

[hXXps://www.linkedin\[.\]com/posts/daniel-grek-sanchez-castellanos-63801262_one-of-the-interview-questions-you-need-to-activity-7270458696927694849-bXRR](https://www.linkedin[.]com/posts/daniel-grek-sanchez-castellanos-63801262_one-of-the-interview-questions-you-need-to-activity-7270458696927694849-bXRR)



Applicant abruptly ends call after being asked to move hand in front of face during interview

Source: LinkedIn

Additionally, subtle indicators such as delayed lip movements, unnatural tone shifts, or inconsistencies across interviews may warrant closer scrutiny.⁸

Behavioral questioning can further support screening efforts. For example, asking candidates location-specific or institution-specific questions about previous employers may help assess authenticity. Where possible, some organizations have opted to include on-site or hybrid interviews as part of their verification protocol prior to finalizing offers.

⁸ [hXXps://www.techtarget\[.\]com/searchsecurity/tip/How-to-detect-deepfakes-manually-and-using-AI](https://www.techtarget.com/searchsecurity/tip/How-to-detect-deepfakes-manually-and-using-AI)

| Insider Threat Detection: Securing the Workforce Post-Hire

Even after successful onboarding, organizations may benefit from implementing ongoing monitoring mechanisms to detect potential insider threats—including those linked to fraudulent hires. One approach used by some security teams is User Activity Monitoring (UAM), which can help identify anomalies such as unusual login patterns, unauthorized data access, or behavioral deviations from baseline activity. For example, multiple geographic logins, attempts to access restricted files, or high-volume data transfers may warrant further review.⁹

Additional security layers may include behavioral biometrics and device tracking. By monitoring elements like keystroke dynamics, mouse movement patterns, and access behavior, organizations may detect indicators of account misuse or shared credentials. If an employee is using remote access tools or virtual private networks (VPNs) to obscure their location, companies should implement geolocation verification to confirm their identity.¹⁰

From a data security perspective, some organizations have adopted Zero Trust Architecture (ZTA) principles to strengthen access management.¹¹ This approach enforces role-based access controls, ensuring employees can only access systems and data necessary for their specific responsibilities—thereby reducing the risk of privilege abuse or unauthorized data exfiltration. Data Loss Prevention (DLP) tools may also support this approach by detecting and blocking unauthorized data transfers, cloud uploads, or outbound email exfiltration attempts.¹² Proactive monitoring of threat intelligence sources—such as dark web forums or credential leak databases—may support early detection of compromised internal credentials. Some organizations have also implemented anonymous insider threat reporting channels to empower employees to flag suspicious behavior without concern for retaliation.

⁹ [hXXps://www.teramind\[.\]co/blog/insider-threat-indicators/](https://www.teramind.com/blog/insider-threat-indicators/)

¹⁰ [hXXps://www.enisa.europa\[.\]eu/publications/remote-id-proofing-good-practices](https://www.enisa.europa[.]eu/publications/remote-id-proofing-good-practices)

¹¹ [hXXps://www.cisa\[.\]gov/sites/default/files/2023-01/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf](https://www.cisa[.]gov/sites/default/files/2023-01/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf)

¹² [hXXps://www.cisa\[.\]gov/sites/default/files/publications/2021-05-26_CDM%2520Data%2520Protection%2520Management%2520Fact%2520Sheet.pdf](https://www.cisa[.]gov/sites/default/files/publications/2021-05-26_CDM%2520Data%2520Protection%2520Management%2520Fact%2520Sheet.pdf)

Finally, workforce awareness remains a key component of long-term resilience. Regular training on fraud tactics, phishing threats, and emerging deception techniques may help employees recognize and report suspicious activity. A strong culture of security awareness contributes to early detection and response while reinforcing shared accountability for risk management.¹³

| Conclusion and Strategic Recommendations

The increasing sophistication of remote IT worker fraud schemes underscores the need for a multi-layered approach to workforce security—beginning with enhanced pre-employment screening and extending into ongoing insider threat detection. Recent disruptions of North Korea-linked fraud operations demonstrate how organizations can be exposed to synthetic identities and deepfake-enabled deception. Financial institutions may be particularly vulnerable given their regulatory obligations, access to sensitive financial data, and reliance on remote technical personnel.

To address these risks, organizations may consider adopting a layered strategy that includes:

- AI and deepfake-resistant hiring protocols incorporating live video interaction, behavioral screening, and open-source identity checks.
- Insider threat monitoring post-hire using behavioral analytics, anomaly detection, role-based access controls, and data loss prevention tools.
- Proactive monitoring of external threat environments, including credential leak databases and dark web forums, to detect early indicators of insider risk.
- Ongoing employee education programs focused on emerging AI-driven deception techniques, phishing tactics, and social engineering threats.

While no single control can eliminate all risk, adopting a layered and adaptive security framework can help reduce exposure to fraudulent remote hiring activity and strengthen organizational resilience against insider threats.

¹³ [hXXps://www.kaseware\[.\]com/post/insider-threats-in-the-age-of-remote-work-unique-challenges-and-solutions-for-remote-environments](https://www.kaseware.com/post/insider-threats-in-the-age-of-remote-work-unique-challenges-and-solutions-for-remote-environments)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%