North Korean Scammers are Posing as IT Freelancers: Here's How You Can Protect Your Business

Insights
5.14.25

Businesses should be aware of growing security risks from North Korean IT workers targeting freelance contracts from businesses in the U.S. and other countries. Typically, these workers fraudulently claim they are from the US or somewhere other than North Korea so they can engage in non-malicious IT work for a business – an activity that is barred by U.S. and United Nations authorities and can have serious consequences for the businesses that accidentally retain them. These workers often gain privileged access to sensitive systems and data through their employment, which can be exploited for malicious purposes, including cyber intrusions and espionage. Here's what you need to know about this fraudulent activity, the potential risks and red flags to watch for, and the steps you can take to protect your business.

Threat Assessment

The federal government has been tracking this issue and providing guidance for years. You can read about the identified threats and potential consequences here: May 16, 2022, October 18, 2023, May 16, 2024, and January 23, 2025.

Notably, North Korean IT workers sometimes work with U.S.-based individuals to provide assistance for their scams, such as:

- A U.S.-based internet connection.
- Acceptance of the company laptop and shipment overseas.
- Financial account setup.
- Attendance at virtual interviews and meetings on behalf of the fraudulent worker.
- Creation of U.S.-based front businesses purporting to offer short-term technical contract workers.

In the FBI's January 2025 guidance, the Bureau points to additional risks of potential extortion and data theft if the fraudulent workers are discovered by the organization. It appears this is a last-ditch effort to gain more funds and is yet another reason to ensure your screening process weeds out fraudulent freelancers.

How widespread is the threat? This type of fraudulent activity can be extensive. For example, on January 23, the US Department of Justice announced the indictment of two North Korean nationals and three facilitators related to this scheme. The scammers apparently obtained work from at least 64 US companies from 2018 to 2024.

Sanction Risks and Reporting

Even unknowingly hiring North Korean IT freelancers can lead to major reputational and legal consequences. Indeed, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned businesses because the money generated from the fraud is being sent back to North Korea's government to support activities such as building unlawful weapons of mass destruction and ballistic missile programs.

You should be aware that OFAC prohibits transactions with individuals or entities on its Specially Designated Nationals and Blocked Persons (SDN) list, which includes certain cybercriminal groups.

If payments are made to sanctioned parties, even unintentionally, organizations may face severe penalties, including fines and reputational damage. This is because OFAC sanctions can be enforced under a strict liability regime, meaning individuals can be held civilly liable for violations even if they did not intend to violate the sanctions or were unaware of them. Criminal liability, however, requires intent or a willful violation, such as conspiracies or attempted violations.

Law enforcement reporting and cooperation, however, can be a mitigating factor considered in any enforcement action that may arise in connection with the payment to a sanctioned entity. The FBI encourages companies to report suspicious activity to the Internet Crime Complaint Center (IC3).

Watch Out for These Red Flags

How can you detect a scam? The guidance provides various indicators including these examples:

- Irregular account access patterns
- Transferring money between connected accounts
- Requesting payment in virtual currency
- Frequent use of remote desktop software
- Repetitive use of document templates
- Unwillingness or inability to appear on camera for video interviews, or inconsistencies during video meetings (such as time or location discrepancies)
- Inability to conduct business during normal working hours
- Social media profiles that don't align with the provided resume
- Rapidly changing home addresses

North Korean IT Worker Scam

Watch Out for These Red Flags

- Irregular account access patterns
- Transferring money between connected accounts
- Requesting payment in virtual currency
- Frequent use of remote desktop software
- Repetitive use of document templates
- Inability to appear on camera for interviews
- Inability to work during normal business hours
- Social media profiles that don't align with resume
- Rapidly changing home addresses

How to Reduce Your Risk

The risk from North Korean IT workers highlights the importance of proper screening to ensure your organization does not fall victim to this fraudulent activity – and companies should adopt vigorous hiring measures to mitigate potential risks. Consider taking the following actions:

- **Educate** HR staff and hiring managers on this threat.
- When using third-party staffing firms, request **documentation of their background check processes** to ensure it is thorough.
- You may want to provide candidates with a release form allowing you **to conduct the background checks directly**.
- **Verify employment and higher education history directly** with the listed companies and educational institutions, using contact information identified through independent research.
- **Request voided checks or certified financial documentation** with account information and verify that checking and routing numbers belong to an actual bank.
- **Use multi-factor methods for identity verification** rather than relying solely on government-issued documents, which can be falsified. Multi-factor processes might involve combining biometric checks (like facial recognition or fingerprints), video interviews, verification codes sent to registered phone numbers or emails, and database cross-referencing to confirm identities.
- Interview candidates **in person** when possible.
- **Utilize video for interviews** to verify appearance with provided documentation, location, and background inconsistences. Just note that North Korean cybercriminals are getting sophisticated with their use of AI deepfake tools to fake identity and infiltrate organizations. Read more about this potential threat here.
- Require candidates to **physically present identification documents** during video verification.
- Ensure **company devices** are delivered with signature confirmation and mailed only to designated work locations.
- Utilize tools to enhance security and verify the location of contractors:
    - Regularly **geo-locate company laptops** to confirm alignment with employee login addresses.
    - Identify when contractors are using **VPNs, proxies, or certain networks** to mask their locations.
    - Consider using **network monitoring tools and endpoint detection software** to monitor network activity, including IP address changes and remote access to ensure logins originate

from approved locations.

- Apply **geo-fencing software** to set location boundaries.
- Utilize **multi-factor authentication** with **location-based authentication**.

- Apply **Zero Trust and Need-to-Know policies**, granting access to proprietary information only when necessary.
- **Review code** to identify instances where it might have been reused improperly or sourced from unapproved locations or to identify unexpected exports of code/data.

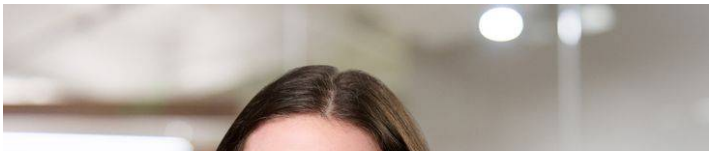
Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Data Protection and Cybersecurity Team. The team is equipped to help organizations implement proactive measures to prevent this type of fraud as well as provide support if fraud is suspected.

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area.

Related People

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email



Jillian Seifrit, CIPP/US
Associate
610.230.6129
Email

Service Focus

Privacy and Cyber

Data Protection and Cybersecurity