FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement

Alert Number: I-101326-PSA | 13 October 2026
North Korean IT Workers Expanding Use of Facilitators, Broadening Recruitment

The Democratic People's Republic of Korea (North Korea) continues to improve its tactics to infiltrate western companies with thousands of state-controlled remote "IT Workers" (ITWs) while avoiding detection. ITWs are increasingly using facilitators to counter improved private sector detections and law enforcement actions. The FBI has observed North Korean ITWs use stolen identities, extort victims, and use threats of physical violence to demand payments. ITWs fund North Korea's government, including its nuclear weapons and other military programs, and pose a significant national security and intellectual property theft insider threat.

The FBI is updating its previous guidance to the public and private sector on techniques and recommendations to identify and avoid this threat. This includes tips to protect yourself and your business, as well as a larger description of how the threat has recently evolved.

The general public needs to be aware that North Korean ITWs increasingly rely on the help of witting and unwitting Americans to acquire jobs in the United States, and they strategically target those under financial stress. ITWs are paying Americans for an expanding range of services to hide their own involvement in the scheme, including asking some to appear on camera, participate in job interviews or meetings, verify fraudulent identities, provide access to personal social media or professional networking accounts, ship packages, complete urinalysis tests or fingerprint submissions, or keep employment-related devices connected to the Internet from personal residences. These actions are illegal, and participating in them puts individuals at risk of law enforcement scrutiny.

U.S. companies should recognize the scale, persistence, and rapid evolution of the North Korean ITW threat means ITWs cannot be identified reliably with a single indicator. Mirroring cybersecurity concepts, detection requires an "identity in depth" approach for effective defense, consisting of multiple layered access controls and detections throughout the employment lifecycle to find, interdict, and remove ITWs regardless of North Korean tactical innovations.

Tips to Protect Yourself as an Individual

For the public, the FBI provides the following information and general recommendations to prevent falling victim to the North Korean ITW scheme.

- Be aware North Korean ITWs post fake job openings on well-known job boards often as freelance gigs with simple requests such as interviewing on

someone's behalf or receiving and hosting laptops in your home.

- ITWs routinely invent elaborate stories, create fake companies, and produce official documentation to lend credibility to their requests. Common ITW backstories include claiming to be Chinese or East Asian nationals in need of a temporary U.S. presence or claiming to be Eastern Europeans displaced by the ongoing Russia-Ukraine war.
- Reject any request to provide personal information, personal details, financial information, or personal account logins in exchange for payment.
- Be aware ITWs have used threats of violence and other acts of intimidation to try to compel Americans to continue illicit activities. If you or someone you know receives a threat to life or is concerned about physical safety, call 911.

Tips to Protect Your Business — Identity in Depth

For companies, the FBI notes North Korean ITWs cannot be identified reliably with a single indicator or detection given the diversity of their activity and significant signature overlaps with legitimate remote employment. Finding ITWs in applicant pipelines or on corporate networks requires examining multiple compounding behaviors that may be innocuous individually, but when considered together are highly suggestive of malicious activity. Listed below are ITW behavioral tendencies and general recommendations.

- ITWs continue to use remote desktop software to connect to employment-related devices. Examples include AnyDesk, TeamViewer, RustDesk, Chrome Remote Desktop, Splashtop Streamer, and remote monitoring and management (RMM) software.
- ITWs use external hardware such as TinyPilot, PiKVM, GL.iNet, and other Keyboard Video Mouse (KVM) over IP devices to control laptops. ITWs have also purchased and used separate laptops to remote into and control employer-provided devices.
- ITWs frequently download applications outside of, or unconnected to their job role on work devices. ITWs abuse open-source software, such as "OBS Studio" with a "VDO.Ninja" plugin (formerly "OBS.Ninja") to establish remote connections, and Homebrew for package management.
- ITWs almost always exfiltrate data since most are mandated to record their screens to track their daily work activity. These recordings are produced on the ITW's device, which can be multiple connections removed from the employer-provided device.
- ITWs tend to rotate through bank accounts, street addresses, social media accounts or other identifiers at an unusually high rate due to account bans and other disruptions.
- ITWs forge verification documents for stolen identities when applying for employment. Using E-Verify, requiring a U.S. passport, multiple forms of identification, or live verification can raise friction for ITWs. Relying solely on "ban lists" or filtering out ITW associated names can be unreliable, block qualified applicants, and risks negatively impacting potential victims of identity theft.

- Cross-functional collaboration between internal teams enhances detection effectiveness. Information technology, human resources, security, and management personnel all have unique insights that when combined can more effectively enumerate ITW activity.
- Implementing aggressive controls against North Korean ITWs presents unusually high risks of generating false positives that could harm legitimate employees and filter out qualified applicants. Balancing the need to disrupt ITWs while supporting legitimate remote employment requires careful detection calibrations, substantive review, and continuous refinement based on observed outcomes.

"Identity in Depth" — layered detections, access controls, and continuous identity verification throughout employment — avoids unreliable filters while enabling moderate, weak, or unavoidable signals to justify enhanced scrutiny when aggregated together. Evaluating identity-related fraud based on probabilistic behavioral data rather than easily bypassed rules provides defenders the resilience and flexibility necessary to counter North Korean ITWs and their ongoing tactical advancements.

Evolution of North Korean IT Worker Tactics

North Korean ITWs collect salaries, steal data, extort victims, and conduct other malicious activities under the direction of the North Korean government,[1] which receives an estimated 85-90% of the revenue the actors generate. This section provides greater detail on how the ITW scheme works and describes some of the latest ITW techniques the FBI has observed.

Facilitator Expansion

Dozens of North Korean ITW teams[2] are hiring Americans and others to complete a wider variety of facilitation tasks, in some cases subcontracting entire jobs to foreign nationals in South Asia or West Africa. ITWs are turning to paid facilitators to avoid improved detections, counter law enforcement disruptions, and maintain more jobs at the same time.

ITWs pay facilitators to keep employment-related devices connected to the Internet from non-alerting locations, such as personal residences, while ITWs remotely access the devices to perform work. These arrangements, often called "laptop farms", have allowed ITWs to obfuscate their locations for years. More recently, ITWs have shifted to maintaining a larger number of laptop farms, with fewer laptops at each to avoid single points of failure.

ITWs pay to use, and apply for employment with, facilitators' social media or professional networking accounts which often contain years of legitimate activity history.

ITWs may recruit and attempt to hire facilitators from impoverished or economically vulnerable populations. Some ITWs have strategized on the best online locations to connect with Americans facing financial stress and have sought out those more likely to complete facilitation requests without question if paid.

Hiring Third-Party Foreign Nationals

Increasingly, North Koreans are obtaining jobs with western companies and then hiring freelancers to complete work assignments for a fraction of the total salary. ITWs subcontract employment-related remote labor to third-party freelancers, usually in Pakistan, India, Nigeria, or neighboring countries.

In addition to remote labor, ITWs hire South Asian or West African freelancers to assist with applying to jobs and with getting hired. ITWs pay these freelancers to apply manually to as many open positions as possible over a given time-period, or to conduct interviews on their behalf.

Given the prevalence of hired third parties, North Korean involvement in fraudulent employment may be hidden or difficult for victims to discern. However, based on FBI investigations over the last several years, North Korea is the only country to devote nation-state level organizational resources, and nationwide technical talent to infiltrating western companies with teams of actors via complex employment fraud.

Identities Used

North Korean ITWs use stolen personally identifiable information (PII) throughout the ITW scheme. Most of the names and addresses ITWs provide to prospective employers are from stolen identities. ITWs also have obtained employment that provided access to sensitive PII, exfiltrated the PII, and used it in furtherance of their schemes.

ITWs pay some facilitators solely to use their identities. ITWs also pay to use the identities of laptop farmers, or facilitators conducting other ITW-related tasks. ITWs use facilitators' identities without permission, or to apply for more jobs than agreed to.

Before using stolen identities to apply for jobs, ITWs often purchase accounts or licenses from identity verification providers to validate and confirm the stolen PII will pass employment background checks. In isolated instances, ITWs have attempted to contact and extort the owners of stolen identities.

Threats of Violence and Escalation Tactics

Recently, the FBI has observed North Korean ITWs use threats of physical violence to demand payments and compel others to take action in support of their scheme. Following termination, ITWs have made death threats against former managers and their families to collect additional payments.

ITWs have threatened to release a victim's sensitive corporate data or publicly post proprietary information unless they received large lump sum payments. ITWs have also threatened victim companies with reputational harm and posted negative information to force further payouts.

ITWs have hired U.S.-based facilitators to appear in-person at victim companies or at the residences of laptop farm operators for intimidation. Facilitators paid by ITWs have also made in-person threats against companies that removed ITW-related accounts.

Targeting Clearance Holders

North Korean ITWs attempt to use identities or facilitators with the qualifications to obtain a larger pool of jobs, including positions requiring U.S. government security clearances or unique technical skills. ITWs target positions with cleared defense contractors and other companies involved in U.S. government contracts.[3] ITWs target active-duty U.S. military members to host laptops.

Impersonations

North Korean ITWs impersonate a wide variety of victims, falsely claiming ownership of social media accounts, professional profiles, and online identities belonging to others. ITWs are increasingly asserting ownership of legitimate tech sector professional networking accounts they have no connection with, for verification purposes or to enhance their applications.

Report It

If you, your company, or someone you know has fallen victim to North Korean ITW activity or has been approached or contacted by a possible ITW, contact your local FBI Field Office and file an IC3 complaint at www.ic3.gov. The FBI recommends including the following information:

- Any legitimate street address reliably connected to ITW activity that received an employment device or is known to send or receive physical items.
- Personal identifiers involved in the activity, including names, social media accounts, phone numbers, emails, bank accounts, IP addresses, professional networking accounts, etc.
- Identifying information on the actor, including images, screenshots, pictures, videos, messages, or documents potentially containing the actor's identity.
- Any details or evidence on facilitators or others potentially involved in the activity.

---

[1]Multiple North Korean government entities operate ITWs to meet budgetary and operational requirements. Examples include North Korea's primary intelligence organization, the Reconnaissance and Intelligence General Bureau, and organizations involved in North Korea's nuclear program. The largest operator of ITWs is likely the Munitions Industry Department under the Central Committee of the Workers Party of Korea which is responsible for North Korea's weapons research, development, procurement, and production.↩

[2]North Korean ITWs operate on teams of around a dozen military aged males under group leaders who report to higher level managers in their parent North Korean state organization.↩

[3]For an example of North Korean ITWs targeting U.S. government contracting positions, see DOJ announcement https://www.justice.gov/opa/pr/maryland-man-sentenced-conspiracy-commit-wire-fraud.↩