外務省 Ministry of Foreign Affairs of Japan | 国家サイバー統括室 National Cybersecurity Office | 警察庁 National Police Agency | 財務省 Ministry of Finance, JAPAN | 経済産業省

Ministry of Foreign Affairs | Australian Government Department of Foreign Affairs and Trade | Global Affairs Canada | Affaires mondiales Canada | Royal Canadian Mounted Police | Gendarmerie royale du Canada

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES — Liberté Égalité Fraternité | Federal Foreign Office | Ministero degli Affari Esteri e della Cooperazione Internazionale | Ministry of Foreign Affairs of the Netherlands | NEW ZEALAND FOREIGN AFFAIRS & TRADE Manatū Aorere

Foreign, Commonwealth & Development Office | Office of Financial Sanctions Implementation HM Treasury

Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers

July 31, 2026

North Korea relies upon a network of skilled Information Technology (IT) workers, deployed within and outside of North Korea, to obtain false identities and remotely earn income to fund North Korea's unlawful nuclear weapons and ballistic missile programs.

North Korean IT workers impersonate nationals of other countries to obtain work and income through online platforms operated by private companies for employment, procurement, and contracting of services. These workers seek out contracts with the intent of remitting their salaries to their parent North Korean agencies. They also pose an insider threat to companies and are involved in data exfiltration, cryptocurrency theft, and theft of sensitive information. North Korean IT workers employ increasingly sophisticated methods, including the integration of AI, to obfuscate their identities and expand their activities globally.

Our countries have repeatedly issued information to warn the international community and private sector of the threat posed by North Korean IT workers. Japan, the United States, and the Republic of Korea issued a "Joint Statement on North Korean IT Workers" in August 2025, and the Multilateral Sanctions Monitoring Team (MSMT) released its second report on North Korea's violation and evasion of UN sanctions through cyber and IT worker activities in October 2025. The United States, Japan, Republic of Korea, United Kingdom, Australia, and Canada have all issued advisories regarding the risk North Korean IT workers pose to private companies, governments, and individual citizens. We continue to actively monitor and counter the North Korean IT worker threat.

According to UN Security Council Resolution 2397, all UN Member States must repatriate to North Korea all North Korean nationals earning income in that Member State's jurisdiction, subject to limited exceptions. Additionally, contracting with North Korean IT workers and paying them for services rendered may also violate the domestic laws of many countries, including Japan, the United States, and the Republic of Korea, and may result in legal consequences or financial penalties.

The Financial Action Task Force (FATF) identifies North Korea as a high-risk jurisdiction subject to a call for action (blacklist). The FATF continuously reiterates the need to implement robust targeted financial sanctions consistent with relevant UN Security Council resolutions and calls on all jurisdictions to apply countermeasures to protect their financial systems from North Korean money laundering, terrorist financing, and proliferation financing risks. Yet, North Korea has increased connectivity with the international financial system through diversified revenue generation activities, including IT worker schemes. As spotlighted in the FATF's Complex Proliferation Financing (PF) and Sanctions Evasion typologies report, North Korea frequently uses IT worker schemes to generate revenue that supports its weapons of mass destruction program.

We urge all countries, companies, and other entities to deepen their understanding of North Korean IT worker schemes and implement measures to counter the tactics listed below. Companies operating online platforms should continue to strengthen their countermeasures, such as enhancing identity verification procedures (strict review of identification documents, requirement of in-person interviews, etc.) and detecting suspicious accounts (introduction of systems that notify anomalous information entries, etc.). The following information is provided by states participating in this alert.

[Modus Operandi Used by North Korean IT Workers]

- Many North Korean IT workers register for accounts on online platforms by falsifying their nationality or identity. Typical methods used include forging identification documents and impersonating another person. North Korean IT workers use images of identification documents provided by third parties—such as proxies residing in third countries—to register accounts, while the actual work is conducted by the North Korean IT workers themselves.
- North Korean IT workers are increasingly likely to use third-party proxies to facilitate the creation of online accounts, participate in job interviews, and even establish in-person contact to create a false sense of trust and obtain work contracts.

- North Korean IT workers often attempt to avoid being paid by direct deposit and may request payment via money transfer services or cryptocurrency. In many cases, North Korean IT workers provide employers a third party's bank account as the recipient for payments, request that the third party transfer the funds to a designated foreign account, and provide a part of the payment to the third-party as a fee for use of their bank account.
- North Korean IT workers often possess high-level skills in IT-related work and are seeking work in wider areas—such as the development of web pages, mobile applications, software, and blockchain applications—through online platforms and other channels. In some cases, they also get work contracts directly from companies or individuals.
- While many North Korean IT workers reside in North Korea, China, and Russia, as well as Southeast Asian and African countries, they may conceal the fact that they are working from abroad using third-party proxies, VPNs, remote desktop software, and similar tools.
- North Korean IT workers are known to use third-party proxies as facilitators overseas, such as in the United States, to run "laptop farms" which receive company-provided laptop computers for North Korean IT workers to remotely access, obfuscating their true location.
- In addition to obtaining IT-related work, North Korean IT workers may obtain foreign currency by engaging in fraudulent foreign exchange trading using automated trading systems they themselves developed.

Furthermore, accounts associated with North Korean IT workers often exhibit the characteristics below. If multiple characteristics apply to a job applicant, there is a possibility that a North Korean IT worker is fraudulently seeking work.

(For companies operating online platforms)

- ✓ Frequent changes to registered information (such as account name, contact details, and bank account information for receiving salaries).
- ✓ The account holder's name does not match the name on the registered payment account.
- ✓ Multiple accounts have been created using the same identification document.
- ✓ Identification documents used for identity verification appear forged or altered using image editing software.
- ✓ Multiple accounts are accessed from the same IP address.
- ✓ A single account is accessed from multiple IP addresses within a short period of time.
- ✓ The account remains logged in for an unusually long period of time.

- ✓ The cumulative work hours or related metrics are unnaturally high.
- ✓ An account user posts false reviews for itself, likely to improve the account's rating.

(For those hiring or procuring services)

- ✓ The account's profile contains errors or uses unnatural expressions that appear to be the result of inaccurate machine translation, indicating a lack of proficiency in the language of the country they claim to be from. (However, North Koreans may use translation services or large language models to produce convincing profiles and communications in second languages.
- ✓ Discrepancies appear in video conference meetings, including photo ID mismatches or video feeds that appear to be manipulated or artificially generated.
- ✓ Refuses to participate in video conference meetings.
- ✓ Offers to work at rates lower than the general market rate.
- ✓ Shows signs that the account is being operated by multiple people. North Korean IT workers often operate in teams, and the individual whom a hiring or procuring official interacts with may change depending on the time of day.
- ✓ Requests payment in cryptocurrency.