

TLP CLEAR

National Cyber Security Centre and New Zealand Police

Cyber Risks of Democratic People's Republic of Korea (DPRK) Information Technology (IT) Workers to New Zealand Organisations

October 2026

Executive Summary

This advisory outlines common practices used by Democratic People's Republic of Korea (DPRK) Information Technology (IT) workers attempting to gain employment from New Zealand organisations, as well as associated red flags, and ways to protect against this activity.

New Zealand organisations are encouraged to review this advisory to better understand and prevent the inadvertent hiring of DPRK IT Workers.

If you suspect this type of activity, please to report to New Zealand Police or the NCSC as soon as possible. Report to Police online at www.police.govt.nz/use-105 , or report a cyber security issue to NCSC at <https://www.ncsc.govt.nz/report/>

Background

The DPRK has deployed thousands of highly skilled IT workers globally. These individuals seek employment in areas such as software development, website design, graphic design, and IT services. The DPRK Government deploys IT workers to gather revenue, including for its nuclear weapon and ballistic missile programmes, as a method of evading UN Sanctions They may also aim to obtain foreign intellectual property to further their own research as well as attempt to steal data for ransom.

The New Zealand Police (NZP) and the National Cyber Security Centre (NCSC) want businesses and organisations to be aware of this risk as there have been instances of DPRK IT workers attempting, and being successful, in obtaining employment in New Zealand and overseas.

New Zealand companies using global contractors may unknowingly onboard DPRK IT workers, especially via freelance platforms.

They are likely to target government agencies, defence contractors, technology companies, financial institutions, large corporates and other businesses with access to sensitive information, critical services, strategic technologies, or international commercial networks.

DPRK workers have been known to target recruitment agencies in order to present a more legitimate persona to potential employees.

New Zealand organisations should take reasonable steps to verify the identity and location of remote workers and be alert to indicators associated with DPRK IT worker networks, including the use of false identities, proxy infrastructure, and requests for payment through third parties or cryptocurrency.

A joint statement was issued by the New Zealand Ministry of Foreign Affairs and Trade (MFAT) on 31 July 2026 about this activity: [Joint statement on North Korean IT Workers | New Zealand Ministry of Foreign Affairs and Trade](#)

How DPRK IT workers operate

North Korean IT workers are part of a state-sponsored cyber strategy aimed at generating revenue and gathering intelligence. These operatives pose as remote freelancers using false identities. Common methods identified include:

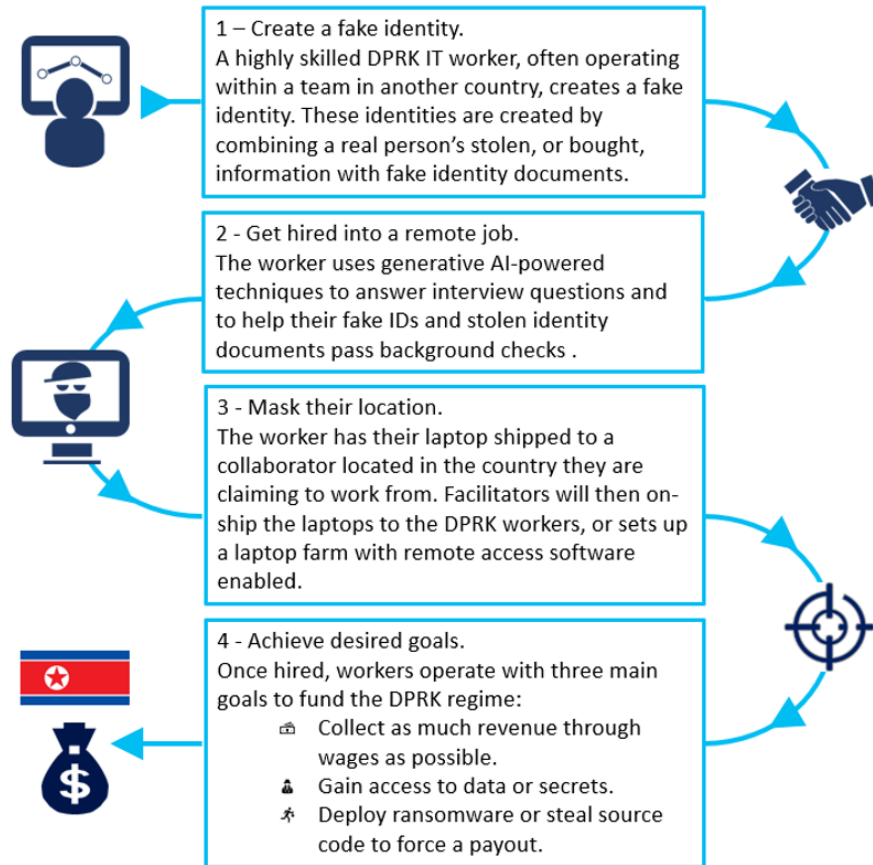
- The use of stolen or purchased identities, sometimes sourced from public registers.
- Creating fabricated CVs, references, and deepfake/AI-assisted interview responses.
- Operating mainly from China, Laos, and Russia, using VPNs and remote-desktop tools to mask location.
- Coordinating through GitHub, Telegram, LinkedIn, Upwork, and other platforms.

In some cases, dismissed workers have sought to maximise financial gain by threatening to disclose proprietary information. This has included attempts to leak sensitive company data or sell it to competitors, creating significant security, commercial, and reputational risks for the targeted organisation.

There have also been instances of New Zealanders unknowingly being used to assist the DPRK workers to obfuscate their identity and location.

- Including:
 - Allowing their New Zealand address to be used for receiving and sending mail, including organisation laptops
 - Logging into the laptops and setting up VPN access for the DPRK worker to appear as if the activity is originating from the laptop and their New Zealand IP address
 - Receiving payments to their New Zealand bank accounts and forwarding to the DPRK worker bank account

Flow chart for how DPRK IT workers operate:



Red flags associated with DPRK IT Workers

While the red flags do not signify illicit activity in and of themselves, they could be indicative of DPRK IT worker activity, especially when two or more are present, and should trigger increased due diligence.

- Identity:
 - Multiple online profiles with different or no photos
 - Request for contact via social media or messaging applications only
 - Refusal to appear on camera, or use of AI masking tools
 - Inconsistent or changing ID details
 - Inconsistent work history or online presence
 - Use of westernised names or pseudonyms
 - Using stolen or doctored New Zealand identities, including drivers' licences and passports
 - The creation of fake business emails to appear as legitimate New Zealand businesses for referee checks
- Location:
 - Requests hardware to be sent to different address from their ID documents

- Accessing an organisations system through remote login instead of using a corporate device provided by the organisation
- Use of remote desktop sharing and control software
- Operating outside declared or expected business hours
- Inability to conduct business during required business hours and inability to reach the worker in a timely manner
- Logged on continuously for more than 24 hours
- Multiple logins into one account from various IP addresses in a relatively short period of time, including IP addresses from different countries
- Payment:
 - Payments made to China-based bank accounts
 - Request to be paid in cryptocurrency or through payment platforms

How can New Zealanders and New Zealand organisations protect against DPRK IT workers?

Steps to protect against the risk of employing a DPRK IT worker:

- Strengthen processes to verify identity and information provided by the IT worker:
 - Check that the name, spelling, nationality, claimed location, contact information, educational history, work history and other details are consistent across the IT worker's application, ID, social media, payment platforms, etc;
 - Consider verifying the identity via an external source;
 - [The Visa Verification Service :: Immigration New Zealand](#) - check if the IT worker has a valid New Zealand working visa if applicable,
 - [Personnel security \(PERSEC\) | Protective Security Requirements](#) and [due-diligence-assessments.pdf](#) contains advice for government departments, however, aspects can be used for any organisation to ensure they are hiring someone with the right to work in New Zealand and conducting due diligence,
 - Do not rely upon external recruitment agencies to provide due diligence for the identity of the IT worker
 - Verifying phone numbers and being suspicious of those identified as being Voice over Internet Protocol (VoIP) numbers;
 - Closely assessing identity documents for evidence of forgery;
 - Verifying documents submitted as part of the application process directly with the education institutions or listed organisations, rather than with contact information provided within the application;
 - Conduct in-person interviews, or require applicants to meet at a local office at some point in the process;
 - Conducting reverse image checks in profile images and monitoring for the use of AI to modify pictures;

- Being suspicious if the IT worker cannot receive mail at the address on their identification documentation;
- If they have claimed previous employment with a New Zealand business or organisation, consider independently verifying the company exists, and that the contact details match those provided by the IT worker.
- Ensure standard business processes are followed:
 - Ensure all hiring procedures are completed and identities are validated by official documentation before granting access rights;
 - Onboarding procedures should not be rushed, and no shortcuts should be taken;
 - Avoid payments in cryptocurrency and require payments be made to a valid New Zealand bank account. Check the bank account details match the IT worker's identity;
 - Require verification of banking information corresponding to their identity documents. Be suspicious of requests for payment to be made into accounts with different names;
 - Be vigilant against requests to communicate outside verified platforms;
 - Limit access to sensitive information using Need to Know policies and utilise access controls and limit permissions.
- Require all workers, but especially those who are remote-only, to use a managed corporate device rather than remote log in from other devices;
- Monitor activity on corporate devices for unusual activity including abnormal access patterns, VPN anomalies or remote desktop applications that could mask geo location;
- Conduct an audit of currently employed remote-only workers to check for any suspicious activity or red flags;
- Report suspicious behaviour to Police or NCSC.

Compliance with New Zealand Sanctions Laws

The DPRK Government deploys IT workers to gather revenue, including for its nuclear weapon and ballistic missile programmes, as a method of evading UN Sanctions.

New Zealand has implemented UN Sanctions on the DPRK through the United Nations Sanctions (Democratic People's Republic of Korea) Regulations 2017. Businesses should be aware of the broad range of prohibitions on dealings with DPRK nationals and entities.

More information about New Zealand's sanctions on the DPRK can be found here: [North Korea | New Zealand Ministry of Foreign Affairs and Trade](#)

Reporting

If you suspect this type of activity, please to report to New Zealand Police or the NCSC **as soon as possible**:

- **Report to Police online at** www.police.govt.nz/use-105, or

- [Report a cyber security issue](#) to NCSC

