Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers

ic3.gov/Media/Y2023/PSA231018

The United States (U.S.) and the Republic of Korea (ROK) are updating previous warnings and guidance to the international community, the private sector, and the public to better understand and guard against the inadvertent recruitment, hiring, and facilitation of Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers. In 2022, the U.S. and ROK Government issued public advisories to provide detailed information on how DPRK IT workers operate, and identified red flag indicators and due diligence measures to help companies avoid hiring DPRK freelance developers and to help freelance and digital payment platforms identify DPRK IT workers abusing their services.

This update identifies new tradecraft used by DPRK IT workers since the release of the 2022 advisories, including new indicators of potential DPRK IT worker activity and additional due diligence measures the international community, private sector, and public can take to prevent the hiring of DPRK IT workers. The hiring or supporting of DPRK IT workers continues to pose many risks, ranging from theft of intellectual property, data, and funds, to reputational harm and legal consequences, including sanctions under U.S., ROK, and United Nations (UN) authorities.

Additional Red Flag Indicators of Potential DPRK IT Worker Activity:

- Unwillingness or inability to appear on camera, conduct video interviews or video meetings; inconsistencies when they do appear on camera, such as time, location, or appearance.
- Undue concern about requirements of a drug test or in person meetings and having the inability to do so.
- Indications of cheating on coding tests or when answering employment questionnaires and interview questions. These can include excessive pausing, stalling, and eye scanning movements indicating reading, and giving incorrect yet plausible-sounding answers.
- Social media and other online profiles that do not match the hired individual's provided resume, multiple online profiles for the same identity with different pictures, or online profiles with no picture.
- Home address for provision of laptops or other company materials is a freight forwarding address or rapidly changes upon hiring.
- Education on resume is listed as universities in China, Japan, Singapore, Malaysia, or other Asian countries with employment almost exclusively in the United States, the Republic of Korea, and Canada.
- Repeated requests for prepayment; anger or aggression when the request is denied.
- Threats to release proprietary source codes if additional payments are not made.
- Account issues at various providers, change of accounts, and requests to use other freelancer companies or different payment methods

- Language preferences are in Korean but the individual claims to be from a non-Korean speaking country or region.

Additional Due Diligence Measures Clients Seeking Freelance Workers Can Consider to Prevent Inadvertent or Unwitting Hiring of DPRK IT Workers:

- If using third party staffing firms or outsourcing companies, request documentation of their background check processes. If this cannot be readily provided by a company, assume it did not conduct the background check and conduct your own.
- If using a staffing company or third-party software developers for IT work, conduct due diligence checks on the individuals the company provides to you for work. Even if you conduct a background on a company, you may not fully understand their background check process.
- Do not accept background check documentation provided by untrusted or unknown authorities. Provide them a release form that allows you to conduct the background check on their behalf instead of having a background check completed by their local authorities.
- Request voided checks or certified documentation from their financial institution with their account information.
- Verify check numbers and routing numbers match an actual bank and do not belong to a money service business. Money service businesses use receiving depository financial institutions (RDFIs), which provide checking and routing information mirroring that of actual banking information.
- Keep records, including recordings of video interviews, of all interactions with potential employees.
- Prevent remote desktop protocol from being used on all company devices and prohibit using remote desktop applications for work.
- Lock down all administrative permissions and install insider threat monitoring software on company devices.
- Require signature delivery for company devices and ensure devices are not mailed to addresses other than designated work locations.
- Require notarized proofs of identity.
- During video verification, require individuals to physically hold driver's licenses, passports, or identification documents up to camera. Consider having them show their location by having the camera directed outside.
- Regularly geo-locate company laptops to verify they match the logins of employees' addresses.
- Require freelancers to shut off commercial VPNs when accessing company networks.
- Use Zero Trust and Need-to-Know policies. Avoid granting access to proprietary information, if possible.
- Use only reputable online freelance platforms that offer robust measures to verify identities and qualifications of freelance workers.
- Avoid recruiting freelance workers directly through online IT competitions and apply reinforced measures to verify their identities.

Reporting

The FBI urges victims of DPRK IT Workers, or those who suspect they may have been victimized, to report the suspicious activity to the FBI Internet Crime Complaint Center (IC3) at ic3.gov.

The ROK government requests suspicious activity be reported to the National Intelligence Service (www.nis.go.kr, 111) and the National Police Agency (ecrm.police.go.kr, 112).

Reference

The original advisory, titled "Guidance on the Democratic People's Republic of Korea Information Technology Workers," can be found here.

The original advisory issued by the ROK government can be found in English here and in Korean here.

For additional information from the Cyber Threat Intelligence Integration Center in the Office of the Director of National Intelligence, please also see "North Korean Tactics, Techniques, and Procedures for Revenue Generation," found here.