ADVISORY ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

The Ministry of Foreign Affairs, Ministry of Science, Information, Communication and Technology, Ministry of Unification, Ministry of Employment and Labor, Fair Trade Commission, National Police Agency, and National Intelligence Service of the Republic of Korea are issuing this joint advisory on December 8, 2022, which requests enhanced due diligence and more stringent identity verification process from domestic companies to avoid hiring or engaging in business contracts with DPRK IT workers who disguise their nationality and identities.

DPRK IT workers are located all around the world, obfuscating their nationality and identities. They earn hundreds of millions of dollars a year by engaging in a wide range of IT development work, including freelance work platforms (websites/applications) and cryptocurrency development, after obtaining freelance employment contracts from companies around the world.

After 2016, North Korea's exports plummeted due to tightened sanctions. As a result, DPRK IT workers' role in earning foreign currency and financing nuclear and missile program for the regime has been ever-growing.

The ROK government preemptively reviewed the identity verification process of freelance work platforms, considering the possibility of DPRK IT workers obtaining employment contracts from domestic companies. Consequently, we concluded that it is indeed possible for DPRK IT workers to obtain employment from domestic companies by obfuscating their identity.

A significant percentage of DPRK IT workers are subordinate to entities which have been designated for sanctions under UN Security Council resolutions, such as Munitions Industry Department and Ministry of National Defense. Moreover, the vast majority of their gross earnings are remitted back to these entities and used for North Korea's nuclear and missile development.

Therefore, the act of offering employment to DPRK IT workers and paying for their work accompanies reputational risks and potential legal consequences for companies, in accordance with relevant domestic

acts, such as the Development of Inter-Korean Relations Act. There is also the possibility of violating relevant UN Security Council resolutions. As such, companies are advised to take extra caution in this regard.

How DPRK IT workers operate

North Korea dispatches thousands of highly skilled IT workers all over the world, including Asia and Africa. IT workers located overseas form groups and live together, and they earn foreign currency by obtaining IT development work via online freelance work platforms.

UNSCR 2397 adopted in December 2017 requires each member state to repatriate all DPRK overseas workers by December 2019. However, these people illicitly and skillfully bypass local authority's surveillance by ditching the work visa to obtain a different type when they enter the country. They then work as an IT worker and earn foreign currency.

They present themselves as non-North Korean nationals and work as freelance IT workers, obtaining employment contracts from companies located in developed countries in North America, Europe and East Asia. These IT workers generate significant amount of revenue by engaging in IT development work, such as mobile applications and software development.

DPRK IT workers are presumed to be engaging in wide-ranging types of work, including the development of Decentralized Applications(DApp), smart contracts and digital tokens, as wells mobile and web-based applications that span a range of fields and sectors, including business, health and fitness, social networking, sports, entertainment, and lifestyle.

Although DPRK IT workers usually obtain employment contract from foreign IT companies and engage in seemingly normal IT work, such as software development, in some cases they are involved in malicious cyber activities, such as obtaining illicit gains by taking advantage of vulnerabilities in smart contract codes. Therefore, domestic blockchain companies must exercise extra caution so as to avoid employing DPRK IT workers.

How DPRK IT workers hide their identity

DPRK IT workers forge their identities and nationality when they look for employment contract and create an account on a freelance work websites.

Forging identification documents is one of the easiest ways to obfuscate their identities. They illicitly collect foreigners' driver's licenses and identification cards, and replace the photos on identification document with their own using Photoshop. Moreover, they utilize a 'proxy phone call authentication service website' when having to going through the process of phone call authentication.

Recently, global freelance work platforms tightened their authentication process, which led DPRK IT workers to borrow freelance work platform accounts from various foreigners in return for distributing certain amount of the generated revenue.

In some instances, DPRK IT workers engage other foreign freelance programmers and establish a business partnership. They collaborate with these non-North Korean freelance workers on projects which were originally commissioned to those workers and split the generated revenue.

DPRK IT workers usually look for targets to borrow proxy accounts via social media. The owners of proxy accounts create accounts on freelance work websites and complete email, phone call, and ID card authentication process for DPRK IT workers. They then provide these authenticated accounts for DPRK IT workers to use.

In order to obtain employment contracts, freelance workers are normally required to carry out the task provided by client companies during the interview. DPRK IT workers favor online text-based chat instead of video interviews. When companies insist on video interviews, DPRK IT workers will show their intermediaries' faces and come up with various excuses, i.e. that they have audio problems due to technical issues. They will then persuade the companies to conduct an interview by phone rather than a video, in which DPRK IT workers themselves will participate in-person. DPRK IT workers are highly skilled when it comes to software development, and some of them are proficient in foreign languages, including English.

Sometimes, even when companies are conducting a real video interview, DPRK IT workers will remotely access the computer of proxy account's owner and demonstrate programming themselves.

The revenue generated via proxy accounts will first be deposited to the proxy's bank account, some of

which will be paid to the owner of the account. The rest of the revenue will be transmitted to local IT team's bank accounts, which are mainly based on global digital payment platforms.

After establishing a business relationship with client companies that commissioned program development, DPRK IT workers typically propose direct communication with clients on a separate platform, instead of the original freelance platform website, thereby minimizing the commission fee for proxy accounts and establishing longstanding business partnership with client companies.

Precautions for IT field contractor platform

If an account on a freelance work platform conforms to many of the characteristics cited below, the account may actually belong to DPRK IT workers. We recommend platforms to take special attention in such cases.

- Multiple logins into one account from various IP addresses in a relatively short period of time;
- Developers are logged into their accounts continuously for a whole day;
- Developers log into multiple accounts on the same platform from one IP address;
- Developer accounts whose cumulative working hours exceed several thousand hours;
- Developer accounts receiving high ratings, especially when client companies which engaged in ratings have a payment account identical to that of the account owner;
- New developer accounts using same or similar documents with those submitted by existing accounts.

We highly recommend IT freelance work platform companies to take tightened measures to verify identity of programmers, such as adding one more authentication step using video call for newly created accounts and requiring client companies to conduct a video interview before signing contracts with freelance programmers.

Precautions for client companies commissioning program development

Client companies commissioning program development are recommended to confirm whether their

partners are DPRK IT workers through stringent authentication procedures.

In particular, if an unknown programmer offers a relatively small development fee, while requesting to communicate via online text-based chat or phone call rather than a video interview, it is highly likely that they are DPRK IT workers or those who are closely related. As such, you should take extra care in having transactions with them.

While conducting a video interview, stringent authentication measures are recommended, such as requiring real ID card during the interview or confirming whether information on identification documents matches information provided for the contract.

When existing cooperation partners are assumed to be involved in identity forgery or related to DPRK IT workers, appropriate due diligence measures, such as video calls without advance notice, can be taken.

Precautions regarding lending accounts

In addition, if an unknown person requests the creation of an account on a freelance IT work platform and a foreign payment platform or asks you to lend a copy of identification documents in return for certain amount of money, they are likely to be DPRK IT workers or those who are related to them. As such, you should exercise extra caution.

Conclusion

We hope this advisory on DPRK IT workers will prove to be helpful in establishing a more secure and reliable online freelance work system and also contribute towards cutting off DPRK's illicit foreign currency revenues which are used for its nuclear and missile development.

Under close cooperation with the international community, the ROK government will continue to raise domestic and international awareness of DPRK IT workers. We will also make further efforts to enhance due diligence of freelance IT work platforms and client companies.

If you have information about illicit DPRK activities, such as DPRK IT workers obfuscating their identities and nationality to obtain employment contracts from domestic companies, please report to police(112), Ministry of Foreign Affairs(02-2100-8149) and other relevant institutions.

ROK Government

Ministry of Foreign Affairs, Ministry of Science, Information, Communication and Technology, Ministry of Unification, Ministry of Employment and Labor, Fair Trade Commission, National Police Agency, and National Intelligence Service