North Korean Tactics, Techniques, and Procedures for Revenue Generation

North Korean IT Worker Red Flag Indicators and Potential Mitigation Measures

KEY: Freelance work or payment processing platforms | Companies hiring the IT workers

STEP ❶: North Korean IT worker purchases proxy account or hires a third party to obscure identity

STEP ❷: North Korean IT worker or proxy submits fraudulent documents or altered credentials on freelance work platforms

Red Flags

- Suspicious account logins
- Remote desktop use
- Fraudulent developer accounts
- Frequent use of document templates
- Suspicious developer ratings
- Extensive project bidding

Mitigation

- Require video verification
- Scrutinize documents for forgery
- Request law enforcement assistance
- Reject low-quality verification images
- Check for workers accessing platform using remote desktop, virtual private network (VPN), or virtual private server (VPS)
- Flag accounts using similar documentation
- Flag developer accounts with high bidding or low-bid acceptance rates
- Do not allow accounts full access without verification
- Scrutinize new accounts

STEP ❸: North Korean IT worker or proxy submits fraudulent documents or altered credentials on digital payment services

Red Flags

- Suspicious account logins
- Remote desktop use
- Frequent money transfers

Mitigation

- Flag accounts that use similar documentation for digital payment services accounts

STEP ❹: North Korean IT worker wins contract from unwitting client on freelance platform

Red Flags

- Requests to use different development or payment services account
- Inconsistencies in provided information
- Overly simple portfolio website or profile
- Direct messages from purported senior executives advertising services
- Requests to communicate on separate platforms

Mitigation

- Conduct video interviews
- Ensure IT worker's information is consistent across profiles
- Conduct preemployment background check
- Do not trust contact information provided by IT worker

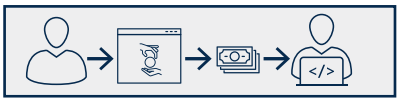
STEP ❺: Client provides equipment to and interacts with North Korean IT worker or proxy

Red Flags

- Developer cannot receive items at listed address

Mitigation

- Disable remote collaboration on computers supplied to IT developers
- Flag IT workers who cannot receive equipment at address listed on their identification documents



STEP ❻: Client processes payments to North Korean IT worker's fraudulent account

Red Flags

- Use of PRC-linked digital payment services
- Requests payment without meeting benchmarks
- Seeks virtual currency payments to avoid know your customer/ anti-money-laundering measures

Mitigation

- Be vigilant for unauthorized, small-scale transactions