KnowBe4

North Korean Fake Employees Are Everywhere!

How to Protect Your Organization

by Roger A. Grimes

Data-Driven Defense Evangelist

North Korean Fake Employees Are Everywhere! How To Protect Your Organization

Table of Contents

It is likely that thousands of organizations around the world are accidentally hiring North Korean fake employees.

INTRODUCTION

On July 23, 2024, KnowBe4 publicly released information about how a North Korean "fake employee" was accidentally hired and detected (https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us).

In some ways, we were lucky, but we worked extremely hard to be prepared for our "luck." We detected the fake employee very quickly after they started to access the laptop we had sent them in unusual ways. We shut down their corporate access within 25 minutes of our first security alert. At no time did they have access to customer data.

After we published our account, several other organizations and law enforcement agencies thanked us for publicly posting about the "North Korean fake employee" problem. It turns out that many other companies had done the same thing but kept their experiences private for various reasons and fears. Our public revelation appears to have opened up a cascade of public information sharing.

> *"Within a few weeks, we heard from over a dozen other companies who either hired North Korean employees or had been besieged by a multitude of fake resumes and applications..."*

Within a few weeks, we heard from over a dozen other companies who either hired North Korean employees or had been besieged by a multitude of fake resumes and applications submitted by North Koreans hoping to get a job with their organization. Many organizations contacting us (or in some cases, we contacted them) asked that we keep their information and experiences private or anonymized, while a few others publicly posted about their own experiences.

It turns out that the North Korean fake employee problem is a complex, industrial, scaled nation-state operation, and it is likely that thousands of organizations around the world have or are now involved in accidentally hiring North Korean fake employees.

Hundreds of U.S. companies have done so. We know of Fortune 500 companies that accidentally hired North Korean fake employees and many much smaller companies (12 employees, 20 employees, etc.) that did the same. It is a serious risk for any company with remote-only employees.

This whitepaper will share what the North Korean fake employee industry is like, share many of the signs of dealing with North Korean fake employees, and discuss many ways organizations can update their hiring policies to prevent hiring such employees.

Note: North Korea is officially known as the Democratic People's Republic of Korea (DPRK).

Legal Consequences of Knowingly Hiring a North Korean Employee

It is illegal for a United States-based or U.S.-located organization (and other United Nations members) to knowingly hire a North Korean due to U.S. law and United Nations (UN) sanctions. In 2017, UN Security Council resolution 2375 (https://main.un.org/securitycouncil/en/s/res/2375-%282017%29) prohibited UN member states and territories from allowing North Koreans to do work for them unless approved in advance by the UN Security Council's 1718 Committee. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has the authority to sanction or fine individuals or organizations knowingly working with North Korean organizations or citizens, through Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501 and North Korea Sanctions Regulations, 31 C.F.R. part 510. In short, anyone knowingly hiring or working with a North Korean person or organization can face very stiff penalties, including jail time and the inability to work with U.S.-based companies and banks.

Note: The U.S. even offers rewards of up to $5M for information on illicit North Korean activities: https://rewardsforjustice.net/index/?north-korea=north-korea.

KnowBe4's North Korean Fake Employee Hire

KnowBe4 needed a principal software engineer for our growing internal IT Artificial Intelligence team. We posted the job on KnowBe4's job website, https://www.knowbe4.com/careers and received, as we always do, a ton of resumes. We reviewed the resumes and conducted multiple interviews. Our finalist job candidate went through four remote Zoom-based interviews with various internal employees, gave references, and sent us a copy of what we thought was an official government identification card. We performed our normal background checks, which at the time were more focused on looking for any past criminal acts or other traditional hiring red flags. We checked references, which were very positive, and after a clear background check, we hired them.

This is who we thought we hired. He called himself **Kyle**.

Whoever was behind the fake employee persona posed as a U.S.-born citizen of Asian ancestry, who was educated in Hong Kong and previously worked at multiple large U.S.-based companies. We soon learned that the name and various identifying information was taken from another real U.S. citizen without their permission. But that real U.S. person's identity passed the previous version of our background checks.

Note: We are not sharing the last name because we want to protect the privacy of the real U.S. citizen.

The picture above was submitted as part of the onboarding process into our corporate and HR systems. The picture is an AI-enhanced version of the person who we interviewed during the hiring process, where the applicant's face was added over a completely different unrelated person's "stock photography" picture so they looked more professional with glasses and wearing formal work attire.

After they accepted the job, we sent them a Mac workstation, which, unknown to the receiver (or simply ignored), contained a lot of good security and monitoring software. We also sent them a multifactor FIDO-enabled YubiKey so they could log into our network. The new employee came up with a plausible excuse so that we would ship the laptop to another location that was not indicated on their resume or other submitted information. As you will soon learn, this is one of the common signs of a North Korean employee.

Every KnowBe4 employee and contractor can only access the applications and data they need to see to perform their roles and tasks. In nearly all instances, this is a very limited set of resources, but more so for new hires. Newly hired employees must take a week or more of training before being released to their team for even more training and oversight as they begin to perform their expected duties.

New employees undergoing training basically have access to corporate email, Zoom, and internal messaging (i.e., Slack), along with a very restricted training system with no access to real customer data. They do not have access to any shared, mapped drives. No confidential data is stored locally on laptops.

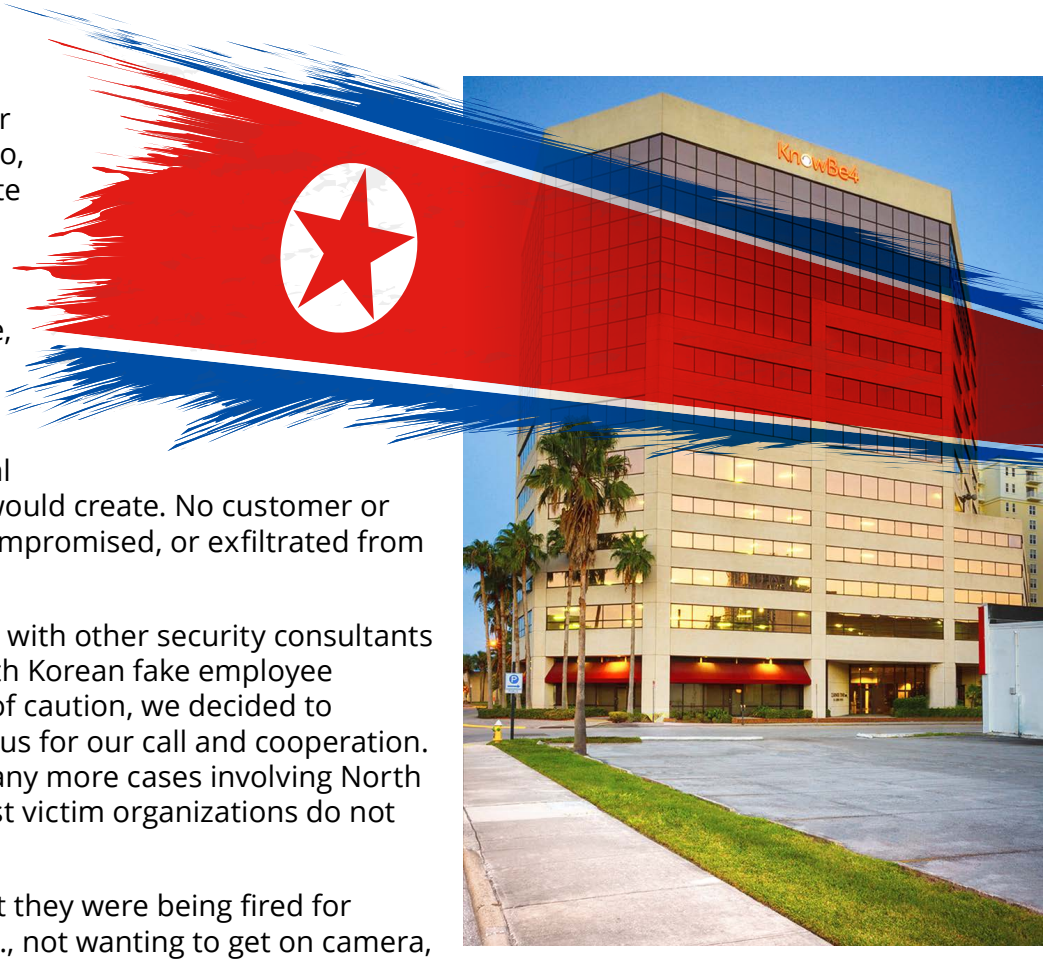
On July 15, 2024, at 9:55 PM EST, the day and time the employee received and powered on the laptop, they tried (and failed multiple times) to install password-stealing malware and manipulate session history logs. At first, they tried to download the malware from a USB device, and when that failed, they tried to do the same using a server located on their local network.

The Mac's endpoint, detection, and response (EDR) software immediately created an alert generated by the attempted malware install. Our InfoSec security operations center (SOC) noted the alert and, within minutes, contacted the new employee using Slack. At this time, our SOC employee did not know we had a North Korean employee situation. They were just reaching out to offer well-meaning help and to see if there could be a legitimate reason why unexpected malware upload and log file change alert messages had been generated.

The person answering the Slack message came back with a strange excuse that did not match the alerts. The remote employee offered up that the alerts were generated while they were troubleshooting a speed issue with their local Internet router. The remote employee's excuses were not making sense, so the SOC employee asked them to get on an audio chat (i.e., Slack huddle) so both sides could more easily discuss what was going on.

The remote employee made an excuse about why they could not get on audio. They eventually stopped communicating on Slack altogether. This immediately triggered a heightened sense of caution in the SOC agent. Within a few minutes, in consultation with other senior InfoSec employees, it was decided to fully isolate the system from our network while logs and additional surveillance information were collected. The laptop was locked down around 10:20 PM EST, 25 minutes from the first alert.

Additional KnowBe4 InfoSec employees were brought in, and they shared the collected data with others at Mandiant, a leading global cybersecurity expert, and the FBI, to corroborate our initial findings. In a short period of time, it was definitively determined that this case had all the signs of a North Korean fake employee scam. We collected as much information as we could remotely from the laptop. We learned a lot about what had been attempted on the laptop as well as useful network information.



We learned that a device running the Raspberry Pi OS was setup to remotely access our laptop as a KVM (Keyboard, Video, Mouse) device, so that the remote North Korean employee and their helpers could access the laptop without alerting our SOC to the presence of a strange, unexpected TCP/IP port traffic that a normal remote access application (e.g., Microsoft Remote Desktop Protocol, Virtual Network Computing, SSH, etc.) would create. No customer or confidential data was viewed, compromised, or exfiltrated from any KnowBe4 service or system.

We eventually came into contact with other security consultants who were well aware of the North Korean fake employee schemes. Out of an abundance of caution, we decided to involve the FBI. The FBI thanked us for our call and cooperation. They said they were aware of many more cases involving North Korean fake employees, but most victim organizations do not report it or cooperate.

We told our new "employee" that they were being fired for violations of company policy (e.g., not wanting to get on camera, unauthorized software installs, etc.) and asked them to send back our laptop. To our surprise, they sent the laptop back, and we turned it over to the FBI. Later on, we learned that other companies who requested their equipment back also got their equipment back. We can only guess the involved perpetrator(s) does not want an additional felony for a stolen equipment charge added to their list of illegalities.

Stu Sjouwerman, CEO of KnowBe4, was made aware of the situation. Once the relevant facts were known and confirmed, Stu (as he is known to everyone), decided to let all employees know what happened. A few days later, at our daily employee meeting, Stu shared what had happened. Another few days later, on July 23, 2024, KnowBe4 publicly released information about how a North Korean "fake employee" was accidentally hired and detected (https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us).

Note: Stu is an unusually transparent CEO. He frequently publicly shares things that most other CEOs would not, like when he had failed a simulated phishing test or that time when he clicked on a real phish (and quickly reported it). People who know Stu or KnowBe4 were not surprised when we shared our latest experience, even though it meant sharing with the world that we had a previous gap in our hiring processes.

Although we did get some early negative feedback from a few critics, the vast majority of responses were overwhelmingly positive. Many people thanked us for being among the first companies to share our North Korean fake employee experience. We got an enormous response to our blog article and dozens of media sources wrote to share our story. Some of the media sources got some of the facts wrong and we subsequently wrote a few more clarifying articles, including these:

https://blog.knowbe4.com/north-korean-fake-it-worker-faq

https://blog.knowbe4.com/how-the-whole-world-now-knows-about-fake-north-korean-it-workers

There is a common long-time complaint in the cybersecurity industry that organizations often do not publicly share when they have been exploited unless required by law, and even then, they often do not include enough useful details to allow other organizations to better protect themselves. This is often because victim companies, rightfully, worry about potential legal consequences of admitting they had a security gap and because they worry about resulting negative publicity or customer responses.

After hearing from many other organizations who had also hired (or almost hired) North Korean fake employees, but had not publicly shared the information, we decided we needed to tell other organizations how to recognize the signs of North Korean fake employees and give suggestions for updating hiring processes. To that end, we created this free whitepaper, created two public webinars, and released more related articles.

If our experience helps other organizations to avoid hiring North Korean fake employees, then we have accomplished our objectives.

BACKGROUND ON NORTH KOREAN FAKE EMPLOYEES

One of the most important points to understand about the North Korean fake employees' scheme is that it is known about, developed, approved, and directed at the highest levels of the DPRK regime, including by DPRK leader Kim Jong Un. The North Korean fake employees' program, often known as the 'DPRK IT workers' in other industry literature, provides a large egress of revenue to North Korea, and in particular to its sanctioned weapons development program, which includes nuclear weapons and other weapons of mass destruction.

North Korea understands the importance that IT and online cyber activities and services play in today's world and in the future success of North Korea. To that end, North Korea has established many schools and universities dedicated to IT skills and cybersecurity. Many of the most promising IT graduates, especially developers with good English-speaking skills, are siphoned off into the North Korean fake employee program.

There are likely thousands of North Koreans involved in the program, both within North Korea and elsewhere. North Korean fake employees are often located outside of North Korea for a bunch of reasons, including the fact that North Korea's Internet IP address space is very limited and known. If North Korea was using Internet access from within North Korea to perform the fake worker

program, it would require more hiding and re-routing or it would be more easily spotted and blocked. On top of that, North Korea has spotty Internet access, frequent power interruptions, and other infrastructure issues that would make such a program harder to accomplish.

Because of these internal infrastructure challenges, North Koreans involved in the fake employee scheme are often located in foreign countries and continents, such as China, Malaysia, Russia, Africa, and other countries in Southeast Asia. China seems to be the most common origination location, likely due to the strong Internet and energy infrastructure, cheaper operating costs, and somewhat similar diets and cultures. Most of the money earned by the North Korean fake employee program is sent back to the North Korean government.

Evolution

It appears that the North Korean fake employee program first evolved from one where they mostly concentrated on gaining "freelancing" work projects on general freelance work websites, such as Fiverr, and from successfully competing for temporary remote work (i.e., contract workers) for companies around the world. This occurred during a time when there was an explosion in the need for more IT workers and developers around the world.

North Korean fake employee work is mostly centered around software and application development work and, to a lesser extent, graphic design. North Korean fake employees often have strong development skills, especially in much sought-after "backend" work, such as interfaces and APIs (application programming interfaces), and in new technologies such as cloud development, cryptocurrencies, and artificial intelligence (AI).

Developers of all kinds, legitimate and otherwise, began to "advertise" their skills and previous work on social media and developer sites, such as LinkedIn and GitHub. It is very common for today's developers to send these links to potential employers along with their resumes, who can look at those sites to see what type of work the employee candidate has done in the past. North Korean fake employees learned how to create simple, but realistic-looking (and fraudulent) resumes and website presences. These fake resumes and websites use fake or stolen identities.

North Korea took advantage of the new WFH jobs being offered throughout the world, moving from mostly freelance work to more full-time positions.

The COVID-19 epidemic (2019 – 2022) accelerated work-from-home (WFH) scenarios where an increasing percentage of employees could work completely remote, often never being required to show up at a physical work location. Today, it is very normal for employers to hire employees without ever having met them or expecting them to meet physically, in person, with anyone in the organization. This is especially true for developer positions. Employers who require that their developers work in the office or in a "hybrid" situation of some in-office days will be cut out of a significant portion of potential employees.

North Korea took advantage of the new WFH jobs being offered throughout the world, moving from mostly freelance work to more full-time positions. North Korean fake employees try to remain employed as long as possible, even though a significant portion are terminated quite quickly due to their discovery of being fake employees or simply poor work performance. Depending on the country and company where the fake employee was working, it can take weeks to months to fire them once someone suspects they are fake. And during this time, they are collecting revenue for North Korea.

Growing Warnings and Other Sources

Even before our personal experience, we were already generally aware of the North Korean fake employee schemes. We even wrote about it here (https://blog.knowbe4.com/fbi-warns-of-north-korean-social-engineering) on October 25, 2023. At the time, we didn't realize the scope, scale, and sophistication of the North Korean fake employee scheme. Most companies did not.

Until fairly recently, the North Koreans mainly pursued positions in cryptocurrency firms, mega-corporations, and freelance work. We also knew our background checks would catch any synthetic (i.e., fake) identities, which were usually created and used in these schemes. North Korean fake employees were notorious for not wanting to be on camera during interviews. We did not count on them using a stolen real U.S. identity, gladly submitting to multiple on-camera interviews, creating AI-enabled pictures, and using fake IDs when needed at physical locations.

How North Korean fake employees operate has changed over time, working to bypass previous successful verification checks, expanding operations, targeting organizations of every type and size, and in their boldness. This is documented over time by government reports and media articles detailing their increasing sophistication and spread.

On May 16, 2022, the U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) released a 16-page detailed report entitled, GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS (https://ofac.treasury.gov/media/923126/download). This report contained tons of details and should be read by anyone interested in this topic. But at the time, because of what North Korean fake employees were mostly doing, the report warned U.S. employers to be aware not to hire fake "freelancers." There was not a huge focus on warning U.S. employers against hiring fake, full-time employees.

As great as the May 2022 report was, it did not receive a lot of media attention at the time. It got lost in all the other reports and articles regarding all kinds of fake employers and fake employees (covered below), popping up during the same period of time.

How North Korean fake employees operate has changed over time, working to bypass previous successful verification checks, expanding operations, targeting organizations of every type and size, and in their boldness.

Nearly another year and a half went by before Mandiant briefly mentioned some signs of North Korean fake employees in a long blog article about all sorts of sophisticated North Korean threats on October 10, 2023 (https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023/). In the article, Mandiant wrote, "...several of the documents focused on resumes, CVs and references, which may be leveraged to apply to various job openings..."

A week later, on October 18, 2023, the FBI updated (https://www.ic3.gov/Media/Y2023/PSA231018) their previous report from May 2022, this time indicating that North Korean fake employee "tradecraft" had evolved to fake full-time employees. This announcement did catch the media's attention, including the KnowBe4 post mentioned above on October 25th. We wrote about the North Korean threat again on December 13, 2023 (https://blog.knowbe4.com/north-korean-operatives-infiltrate-job-platforms) based on a new report from Nisos (https://www.nisos.com/research/dprk-it-worker-scam/).

Mandiant started to be involved in more and more cases of North Korean fake employees. Mandiant Principal Analyst, Michael Barnhart, joined The Defender's Advantage podcast (https://open.spotify.com/episode/0xeaavXjlX2XLm3oibOv6g) on February 21st, 2024, to talk about the problem.

By May 2024, the problem was becoming more well-known outside of cybersecurity circles. The Wall Street Journal revealed (https://www.wsj.com/politics/national-security/american-it-scammer-helped-north-korea-fund-nuclear-weapons-program-u-s-says-65430aa7) that over 300 U.S. companies had hired North Korean fake employees and revealed that Americans and other foreign nationals were assisting them. On June 7, 2024, the Wall Street Journal published another related article entitled, "Deepfakes, Fraudsters and Hackers Are Coming for Cybersecurity Jobs" (https://www.wsj.com/articles/deepfakes-fraudsters-and-hackers-are-coming-for-cybersecurity-jobs-e2a76d06).

What was often missing in the media reports was an abundance of details of what the fake employee candidate did during the interview process to fool unsuspecting firms. While different types of organizations were sometimes mentioned (e.g., a major television network, an aerospace and defense company, a car manufacturer, etc.), the focus again was often on mega-corporations hiring freelancers and did not mention that smaller companies…sometimes very small companies…were also being targeted. They did not mention people getting on camera. It is more difficult to defend when the relevant details and recommended defenses are not being readily shared. And until recently, none of the news stories went "viral" and really gained worldwide traction. Most organizations were unaware of the scale and sophistication of the North Korean fake employee problem.

That changed with our July 23, 2024 blog post. We publicly shared details, pictures, security gaps, and suggested defenses. And it worked. There were dozens of news articles the next day, and now more companies feel comfortable publicly sharing their own North Korean fake employee experiences.

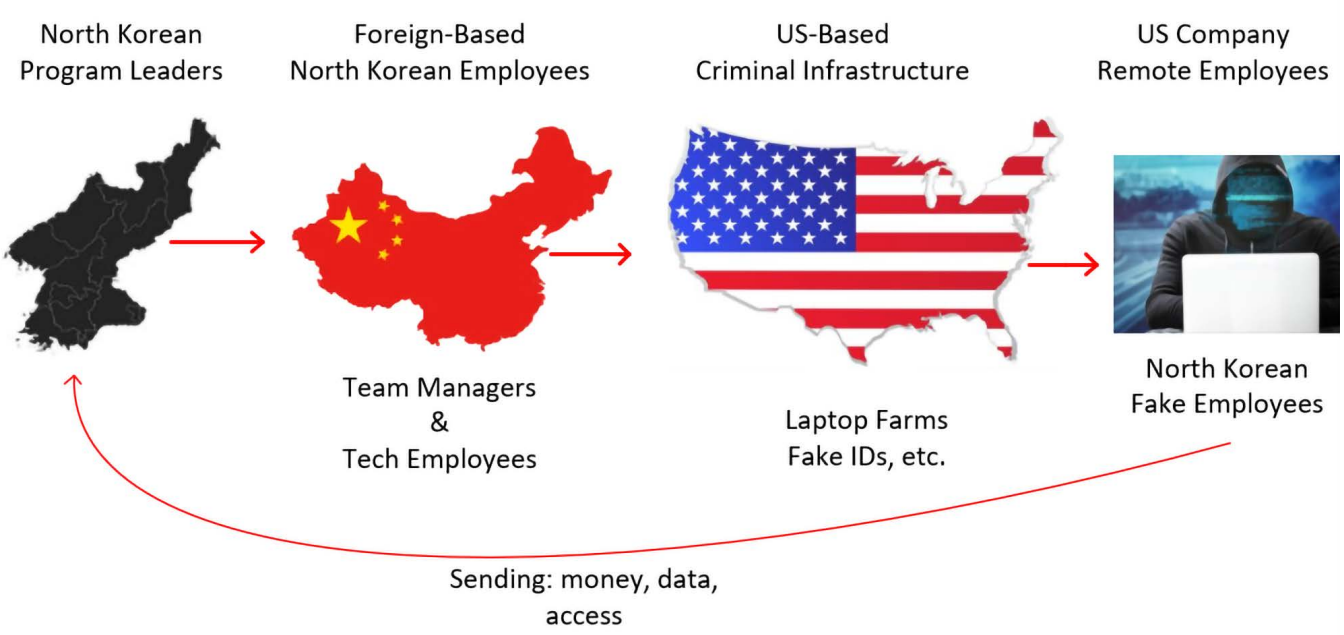
You can use background services that will confirm whether or not the employee you are thinking of hiring is or is not a North Korean fake employee. There is a smattering of free tools anyone can use to do some Open Source Intelligence (OSInt) investigations on their own, including https://github.com/shortdoom/gh-fake-analyzer/tree/main#malicious-github-accounts. Individuals are even sharing (https://github.com/shortdoom/gh-fake-analyzer/blob/main/profiles/INVESTIGATIONS/ZachXBT_15.08.2024/Attackers.jpeg) names, email addresses, and IDs of proven North Korean fake employees. North Korean fake employees often have many jobs at different organizations using the same fake or stolen ID, so knowing the names of the confirmed fake employees can help organizations avoid being duped.

Note: It would be extremely helpful if a government's website had a "global list" of all confirmed North Korean fake employee names and ID information where they all could be easily shared or queried by anyone.

The U.S. Department of Justice has announced several separate charges and arrests of U.S. citizens and other foreign nationals who are helping the North Koreans with their fake employee schemes, including an Arizona woman and Ukrainian man here (https://www.justice.gov/usao-dc/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north) and a Tennessee man here (https://cyberscoop.com/wp-content/uploads/sites/3/2024/08/FILED-INDICTMENT-Knoot.pdf).

It is our hope that more and more organizations will share their experiences with North Korean fake employees, and really, any exploitation, so that we can all learn together and better protect ourselves.

General Infrastructure



There are four general parts to the North Korean fake employee scheme:

- North Korean-based program leaders
- North Korean employees and managers based in other countries
- Non-Korean scheme assisters (usually based in the country where the job is located)
- Infrastructure to assist with accepting payments, generating fake identities or stealing real identities, creating fake employee websites and projects, giving references, money laundering, document forgery services, etc.

The North Korean fake employees are often skilled IT workers and developers trained at North Korean universities. They are usually located in foreign countries, such as China, in shared apartments (living spaces) and workspaces. The daily work is usually performed in a room that looks like a busy call center. In fact, many of the potential employers noted the noisy background any time they interviewed the employee candidate.

Most of the money earned by the North Korean fake employees is sent back to the North Korean government. The local manager (or minder) takes a small portion of the proceeds first for themselves and operations before remitting the rest back to North Korea. The North Korean employee gets very little of the earned revenue. It is believed that their close family members are always kept back in North Korea to be used as personal leverage to force the employee to toil long hours for very little wages. Several sources have concluded that North Korean fake employees are considered to be “human-trafficked”.

There is a large criminal ecosystem of support services that assist the North Koreans with their fake employee schemes. The North Korean fake employees will use fake, stolen, or purchased identities. Stolen or purchased identities will often be from the country being targeted.

North Korean fake employees often create or obtain fake "official" documents when requested by the employer. According to the FBI (https://ofac.treasury.gov/media/923126/download), previously submitted forged documents have included:

- Driver's licenses
- Social Security cards
- Passports
- National identification cards
- Resident foreigner cards
- High school and university diplomas
- Work visas
- Credit card, bank, and utility statements

Stolen or purchased identities are preferred because they more easily meet the job requirements and pass background and other checks. In some cases, the owners of the real identity have been paid to assist in the scheme, participating in interviews, picking up equipment, and taking drug tests. Other times, it is other unrelated individuals pretending to be the other identity, often using fraudulently created, official-looking IDs.

As documented in several judicial proceedings (including here: https://www.justice.gov/usao-dc/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north), there are many services and websites worldwide which, knowingly or unknowingly provide stolen identities to the North Koreans. Some reports have described services and websites (and Discord servers), which offer U.S. citizens a chance to earn money by being part of the scheme. It appears that sometimes the involved citizens think they are helping foreigners get jobs they would otherwise be "discriminated against" obtaining. And in other cases, they do know they are involved in helping North Koreans bypass sanctions.

Laptop Farms

There are usually citizens in the same country as the job position to accept equipment mailed by the employer. They often set up the equipment in their homes and other locations so that the remote North Koreans (or their hired contractors) can access the equipment. One "laptop farm" was found with over 90 different laptops from various employers. Several employers receiving the equipment back after firing the fake employee have reported that the laptop lid contained a yellow "sticky note" with the name of their organization inked on it. It is obvious that the laptop farm employee was labeling the equipment to keep track of which laptop belonged to which organization.

North Koreans, after learning they have been accepted for a new position, almost always tell the employer to ship the laptop and other equipment to another location not previously disclosed on their resume or other systems. This is a very common sign of a North Korean fake employee. They come up with various fake excuses, such as new permanent living locations, helping out a sick relative, and traveling with a girlfriend. Regardless of the excuse, the new location to which they ask for the equipment to be mailed is usually unknown and a surprise to the employer.

This is likely because the North Korean employee is involved in dozens to hundreds of ongoing fake employment schemes, and when accepted for new employment, now has to direct the employer's equipment to a valid local country equipment farm. These laptop farm managers do quit and get arrested, so the North Koreans are using a forever-changing list of laptop farmers.

Note: It is likely that in the future, because this tactic has been publicly revealed, the mailing location the laptop is shipped to will be used early and consistently in the job application process. This and other current signs of a North Korean fake employee may change as the North Koreans respond to publicly revealed tactics and successful defender mitigations.

The equipment handlers often have fake IDs in the name of the fake hired employee, but with their picture inserted for the visual review. Employers shipping equipment to remote employees should ensure that the person picking up the equipment visually and informationally matches the person who participated in the previous hiring processes. The North Koreans rely on the fact that most of the legitimate services involved in checking IDs are not comparing the IDs they receive with each other, for if they did, they would see distinct differences in most cases (except where a single fake employee is participating in all aspects of the scheme).

There are North Korean fake employee schemes where a country's citizen is thoroughly involved in the employment scam, from using a real resume, participating in the interviews, taking drug tests, picking up the equipment, etc., and then turning over the resulting work and the rest of the interfacing to the remote North Korean worker (or the contractor they hired).

North Korean fake employees will often turn over the resulting work to other foreign and domestic contractors. They will either let the contractor take over part or all aspects of the fake employee scheme and earn a percentage of the paid salary. Some employers have noted that the person they thought they hired was not the person doing the work, either in physical looks, voice/accent, or the related knowledge and/or quality of work delivered. Other times, the North Korean fake employee does all the work except pick up the corporate equipment.

There is often an entire ecosystem of supporting criminal services and people involved. The services include fraudulent identity services, fake banks, money laundering, cryptocurrency services, cryptocurrency exchanges and "mixers", "mules", laptop farmers, subcontractors, resume writers, social media and GitHub account creators, developers, job finders, fake ID creators, VPN services, VOIP services, etc. Those involved often know that what is being done is illegal or unethical, but may or may not know that North Korea is involved.

It can be assumed that North Korean employees within the same managed group, and possibly at larger levels, share what tactics do and do not work. They likely share what caused failures, how to possibly bypass them, and what ecosystem services made their jobs easier and more successful.

They likely use different techniques for different scenarios, depending on what types of defenses they have to overcome.

The North Koreans largely depend on employers not being aware of the threat and not implementing defenses that can detect and prevent them. The revenue earned by North Korean fake employees results in hundreds of millions to billions of dollars reaching the North Korean government, much of which is used to fund their sanctioned weapons programs.

Inbound/Outbound Strategies

Many organizations report "inbound" contact with North Korean fake employees, where the North Korean employee reached out to the employer about a possible job. That contact was initiated from a job offered on the employer's website or from a legitimate job's website. In a few cases, the North Korean fake employee reached out to a developer manager on social media (e.g., LinkedIn, etc.) and inquired if any jobs were available.

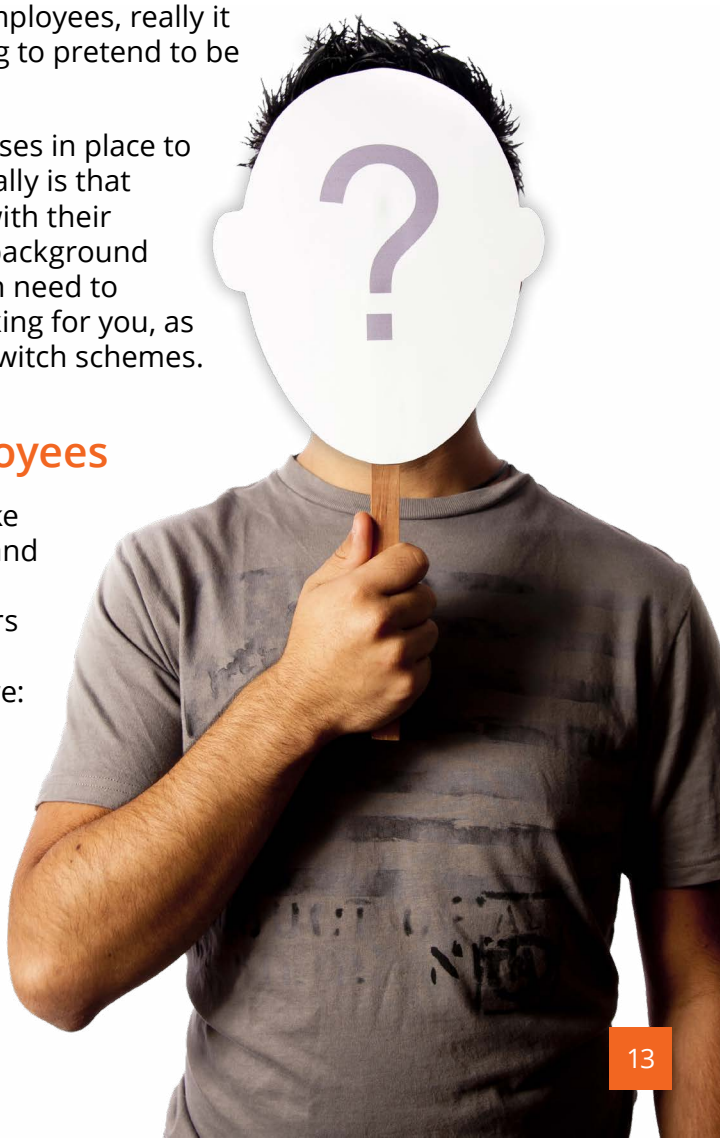
In many other cases, the employer reached out (i.e., outbound) to the North Korean fake employee, not knowing they were North Koreans or fake profiles. In most of these cases, the North Koreans hosted basic, but credible profiles on social media, GitHub, or other seeking jobs websites. In some cases, the employer actively looked for potential employees on LinkedIn and came across fake profiles.

Recruiters often played a big role in both inbound and outbound contacts with North Korean fake employees. Many employers were brought the North Korean fake employee by a trusted recruiter who had previously, unknowingly, been duped. Every recently interviewed recruiter reported a very large, serious problem in the recruitment industry from North Korean fake employees.

Many employers reported both multiple inbound and outbound contacts with North Korean fake employees over the last year, but only now, knowing the signs to look for, realized they were North Korean fake employees.

Fake remote employees and contractors are now something every organization needs to worry about. Every organization should be updating its hiring policies and training to reflect this new reality. While the news is all about fake North Korean employees, really it could be from any country and really any person wishing to pretend to be someone else.

At the very least, every organization should have processes in place to confirm the identity of the person they intend to hire really is that person, whether that is meeting them in person along with their government-issued ID or using trusted agents, such as background searching firms, which include relevant checks. You even need to ensure the remote person you hired is still the one working for you, as many remote employee scams have involved bait-and-switch schemes.



Other Fake Employers and Fake Employees

Readers should understand that fake employers and fake employees abound and are not just a problem created and solely operated by North Korea. For over a decade, the cybersecurity industry has noted a raff of fake employers and fake employees (including from North Korea), and KnowBe4 has written about it many times, including here:

https://blog.knowbe4.com/fbi-scammers-exploit-job-posting-sites-with-fake-jobs-to-steal-money-and-personal-information

https://www.securityinfowatch.com/security-executives/article/53079753/the-dilemma-of-fake-job-scams-is-hard-to-stop-at-scale

https://www.linkedin.com/pulse/how-stop-job-scams-roger-grimes

https://blog.knowbe4.com/job-seekers-and-employers-beware

https://blog.knowbe4.com/north-korean-threat-actors-target-software-developers

https://blog.knowbe4.com/heads-up-north-korean-cybercriminals-use-fake-recruitment-emails-in-phishing-scam

https://blog.knowbe4.com/how-nks-cyber-criminals-stole-3-billion-in-crypto-to-fund-their-nukes

The FBI has warned about fake employers looking to harm individuals many times in the past, including here:

https://www.ic3.gov/Media/Y2024/PSA240604

https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-warns-cyber-criminals-are-using-fake-job-listings-to-target-applicants-personally-identifiable-information

https://www.fbi.gov/contact-us/field-offices/newhaven/news/press-releases/fbi-new-haven-warning-college-students-of-employment-scams

It should be noted that many fake jobs are advertised on legitimate job websites. The North Koreans and others fool legitimate job sites into posting fake job ads, which often add an air of legitimacy to the posted job. Certainly, anyone not suspecting that a potential advertised job is fake is at far greater risk of falling for the employment scheme. The legitimate job websites often look for and weed out fake employment ads, but it is often a losing game of cat-and-mouse.

Many countries, including Iran, south Asian countries, and Russia, seem to have many sophisticated groups dedicated to pretending to be fake employers and employees. Fake employers are also very problematic. These fake employers often target already working employees, hoping to steal something of monetary value from the victim (by making them pay fake pre-employment fees or purchase and ship expensive equipment to get the job) or to target their existing employer. Employees have been compromised, so the attacker could gain access to the employer to spread malware, ransomware, steal money, or obtain confidential information.

One of the most infamous cases is where a fake LinkedIn job ad enticed an existing employee of a cryptocurrency firm to apply for the fake job and ended up resulting in his current employer being robbed of $500M in cryptocurrency: https://www.techtimes.com/articles/277721/20220706/axie-infinity-hacked-500m-lost-via-fake-linkedin-job-listing.htm. The culprit in this case was the Lazurus group, a well-known North Korean nation-state hacking group.

Your hiring process should include mitigations to prevent all sorts of fake employees.
All employees in the hiring process should be educated about fake employees. All employees should be educated about fake employer scams too, as they can result in personal harm and harm to the organization.

Intentions

The U.S. government has repeatedly stated that the main intention of the North Korean fake employee program is to provide illegal revenue to North Korea through the receiving of work payments, such as salaries and other contractual payments. The vast majority of reviewed information from involved activity logs and interactions shows that most of the time, the fake employee simply performed the type of work they were hired to do and thus earned continued compensation. In other instances, they did not perform the required work (or performed it poorly or rarely), but did not perform other malicious or espionage activities. The main intent of the North Korean fake employee program seems to be to collect continued revenue over extended periods of time, often then used for the sanctioned North Korean weapons programs.

At the same time, there are many confirmed instances in which the infiltration of North Korean fake employees also led to monetary theft by other means, such as stolen cryptocurrency or malicious corporate bank transfers. There have been many cases involving the exfiltration of confidential information, intellectual property, and project secrets. There have also been cases of malicious code intentionally inserted in the software projects in which the North Korean fake employees were involved.

It is believed that many of these instances are cases where the involved handlers recognized the significance of the compromise in regard to the larger interests of North Korea and in some cases, specific organizations and industries were likely intentionally targeted with specific espionage goals in mind.

In the absence of information to the contrary, any exfiltrated company should assume that goals beyond revenue may be involved. With that being said, the vast majority of investigated cases had the main intent of earning revenue through work efforts. Potential victims should install and manage strong monitoring systems on involved endpoints to be able to collect data to prove intent and detect all worker actions, if needed, during a potential compromise.

The rest of this whitepaper is the real meat, covering the signs of a North Korean fake employee and how employers should update their hiring processes to protect their organization.

SIGNS OF A NORTH KOREAN FAKE EMPLOYEE

Here are some of the common signs of a North Korean fake employee:

During the Hiring Process

- Presents themselves as Asian (e.g., South Korean, Chinese, Malaysian, Japanese, etc.), European, or U.S.-based
- Will often claim to have always lived in the U.S., to have only gone to U.S.-based universities, and worked for well-known U.S.-based companies, even though their English is limited
- Will often claim to be a U.S.-based citizen with an American/English-sounding name, but will have a very heavy accent
- If you are familiar with Asian accents, the accent will often not be from the claimed country or region (will often be a North Korean accent)
- Will often use a fake identity that will fail if checked
- Will often submit a fake ID credential that will fail if checked
- Will often claim a fake work history that will fail if checked

- Supplied personal websites, profiles, or GitHub sites seem overly basic, often saying something and nothing at the same time or you can find very similar sites and profiles
- Often claimed prior work product can be tied to other names
- Sites and profiles are relatively new or match the date when various "former" work products were created/posted
- Claimed identity has zero Internet presence or history outside of supplied sites and profiles
- Conflicting inconsistent information provided between resumes, social media sites, profiles, in interviews, and how they answer questions or what they select or input on HR hiring systems (such as marital status, address, etc.)
- All connections are made using VPNs
- Candidate will participate in interviews from a noisy (call center-like) background
- All phone numbers submitted (candidate and reference) will be virtual voice-over-IP (VoIP) numbers (which can be checked online)
- Candidate and reference email addresses will always be email addresses from commonly used public email domains (e.g., Gmail.com, Hotmail.com, Outlook.com, etc.)
- Reference phone numbers and email addresses will never be to legitimate business phone numbers or email domains of the claimed business
- May be hesitant coming on camera for one or more interviews, may make excuses for why camera is not working

After Hiring

- Wants you to mail organization devices to an additional location not indicated on the employment application or in previous communications
- You detect unnecessary remote login on the organization's device
- IP address where the organizational device is logging in from does not match the claimed location
- You detect malware on the organizational device
- You detect unusual behavior on the organizational device
- Changes to log files or other cover-up attempts on the organizational device
- Work hours do not seem consistent with the country or region being claimed, emails and work product seem always to be delivered during very late night hours
- Minor misspellings on things they should not be misspelling (like their name, address, etc.)
- Frequently changing email addresses (because they have been detected and shutdown on the old email address)
- Inconsistent project delivery quality, definitely does not seem to meet the quality of person interviewed
- Inability to get them on camera or inability to get timely responses from online channels, especially during hours that would be sleeping time for them
- Unusual/strange payment scheme requests, especially using virtual currency
- If they request that work payment be sent to a bank, banking details provided for payment are to a strange-looking bank or do not match public records
- They request that payments be made to virtual currency, cryptocurrency, or other popular money exchange sites (e.g., PayPal, Venmo, etc.)
- Employee changes OS or application to Korean language support even though the claim to be of another nationality

An employee candidate does not need to match all these common signs to be a fake employee. But it is good to create checks for each of these and if any candidate being considered as a finalist meets even some of these signs, they should be further scrutinized and reviewed for accuracy before continuing. Most employers who eventually detected a North Korean fake employee or resume, when checking past submissions, found additional likely North Korean fake employee candidates (who had not made it through the normal hiring process to become a finalist).

HOW TO PROTECT YOUR ORGANIZATION

Fake employees, North Korean and otherwise, are a serious threat to every employer, especially those with remote-only positions. Every at-risk organization should educate all employees who could be involved in the hiring process about the risk and consider following the various mitigations listed below:

During Hiring Process

- Share the risk with senior management, if they are not already aware, and obtain senior management support
- Threat model your hiring process
- Update your hiring process to mitigate the risk of hiring fake employees
- Share the signs of potentially fake employees with those in the hiring process
- Run existing remote-only employees through a process to ensure that you do not have an existing fake employee
- If possible, always require that remote employees physically meet with an employee, team leader, or selected agent of the organization in person, with an official ID, to confirm they are who they say they are
- If not already existing, create a rule that all employee candidates and employees must always be on camera during remote sessions (e.g., Zoom, Microsoft Teams, Slack, etc.)
- Keep a record of all interactions and videos of the interview process
- If possible and reasonable, and if the employee candidate has a non-domestic accent, have a trusted person who is familiar with accents from the same region participate in a meeting to assess the validity of the claimed accent
- Check for VoIP phone number use from employee candidates and references
- Check references
- Require that all professional/work references be made to legitimate and publicly confirmable business phone numbers and email addresses (do not allow generic public email addresses only)
- Use a background check that looks for fake employees
- Require that candidate use the same ID when presented to anyone in the hiring process and make sure additional identity verifiers in the process get a copy of the first submitted identification
- Ask the candidate to submit fingerprints for identity verification purposes

Optional: This last suggestion is not really that conclusive, but several people in the hiring process who ended up detecting a North Korean fake employee used this type of questioning to determine if the employee candidate was really who they said they were when they were becoming suspicious. If skeptical, ask a question that the candidate should easily know if being honest, but it is not super easy to quickly look up the answer. For example:

- If the employee candidate said they went to Virginia Tech, ask them, "What is a Hokie" or "What's that song that the football team always enters the stadium to?"
- If the employee candidate states they worked for a particular employer one of the reviewers also worked for, ask a question that anyone who worked for that employer should readily know. For example, "You worked for Microsoft; what color badge did you have?" Any real Microsoft employee would easily tell you the right color for the employee type.
- "What was the name of that mascot for the baseball team?"
- "What score did you score on your SATs?"
- "What was the name of that huge student information center located on campus?"
- "What was the name of that bar located next to campus that everyone went to?"
- "What was the name of that main road running right in front of the campus?"
- "What food is considered the primary food eaten at baseball games?"
- "Do you have an HOA where you live?"
- "Did you have to register for Selective Service?"
- "At what age did they allow you to get a driver's permit (in that state)?"
- "Oh, I see you worked at Autodesk. What type of internal instant messaging system did they use, again?"

Realistically, if you are becoming that skeptical during the interview process, perhaps they should not be considered as a finalist for that position.

After Hiring

- Lock down any supplied device to the bare minimum access needed, especially during the initial hiring period
- Monitor device for unusual activity, malware, unexpected language changes, or log modifications
- Look for signs of unexpected remote logins
- Consider asking them the same technical questions you asked during the hiring process to see if their answers match what they gave during the interview
- Monitor activity against purported normal work hours
- Require employee to be on camera during training or any time when communicating with another employee
- Randomly ask the employee to come on camera a few times, at least during the initial employment period

Note: The FBI encourages U.S. companies to report fake employees to their local FBI field office.

SUMMARY

Fake remote employees and contractors are now something everyone needs to worry about. Every organization should be updating its hiring policies, processes, and education to reflect this new reality.

While the recent news is all about fake North Korean employees, really it could be from any country and really any person wishing to pretend to be someone else. At the very least, every organization should have processes in place to confirm the identity of the person they intend to hire is really that person, whether that is meeting them in person along with their government-issued ID or using trusted agents, such as background searching firms which include relevant checks. You even need to ensure the person you hired is still the one who is working for you, as many employee scams have involved bait-and-switch schemes.

We used to live in a world where we did not have to worry about fake employees or employers. But times have changed and hiring processes and employees seeking new jobs need to act accordingly.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 70,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E09K01