KnowBe4
Human error. Conquered.

North Korea's Secret IT Army and How to Combat It

Roger A. Grimes, Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com

Roger A. Grimes

Data-Driven Defense Evangelist

KnowBe4, Inc.

e: rogerg@knowbe4.com

Twitter: @RogerAGrimes

LinkedIn: https://www.linkedin.com/in/rogeragrimes/

Mastodon: https://infosec.exchange/@rogeragrimes

Bluesky: rogeragrimes@bsky.social

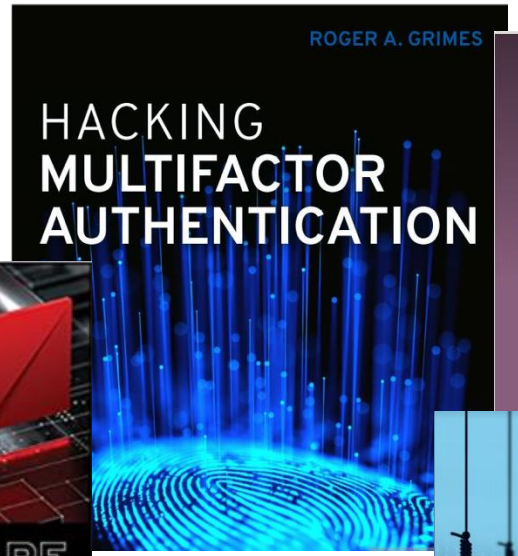
About Roger

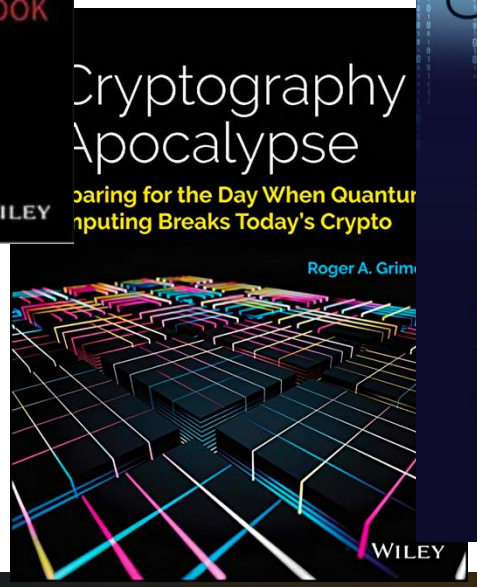
- 35 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 14 books and over 1,400 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g., Newsweek) and radio shows (e.g., NPR's All Things Considered)

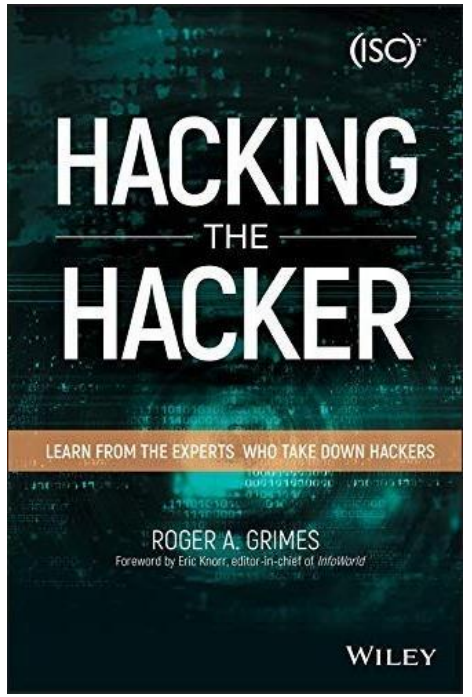
Certification exams passed include:

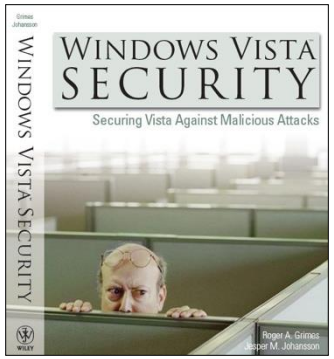
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

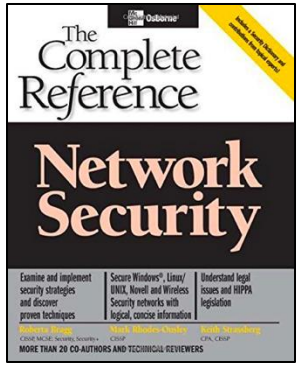
Roger's Books

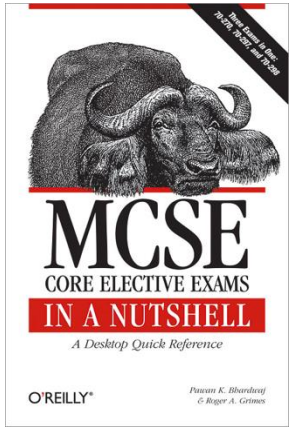


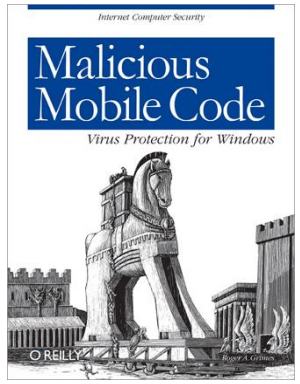


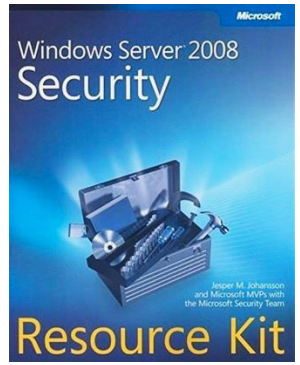


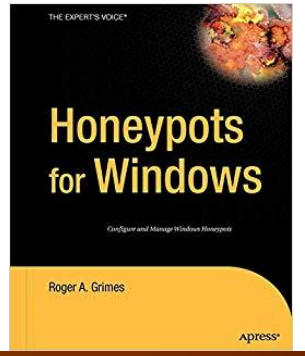








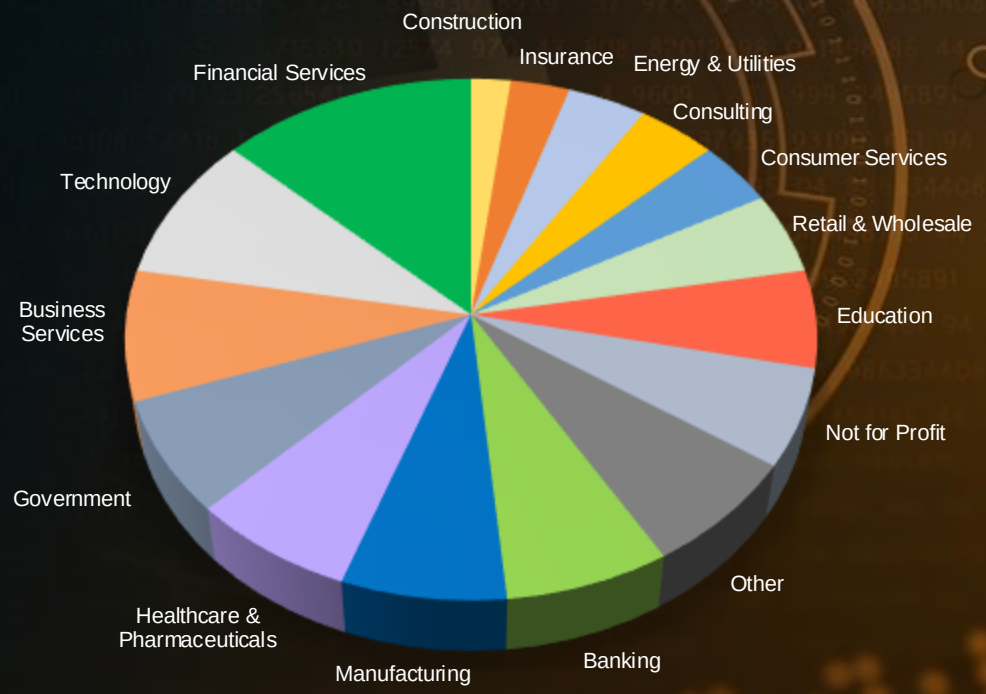




Over

70,000

Customers



About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

Agenda

- KnowBe4's North Korean Fake Employee
- Background/Ecosystem
- Signs of a North Korean Fake Employee
- How to Defend

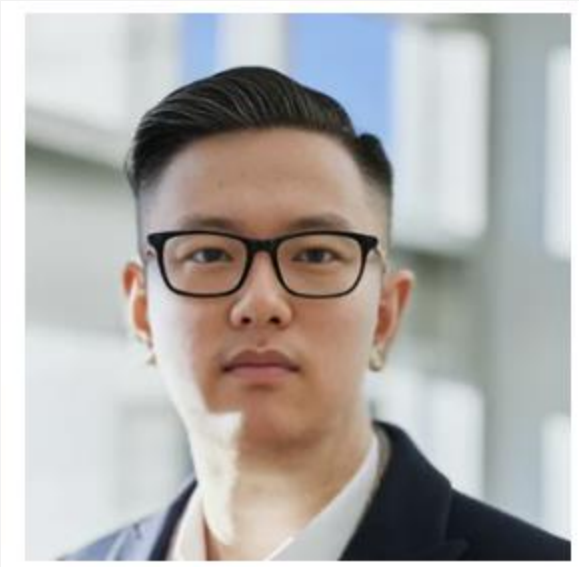
KnowBe4's North Korean Fake Employee

KnowBe4

KnowBe4 North Korean Fake Employee

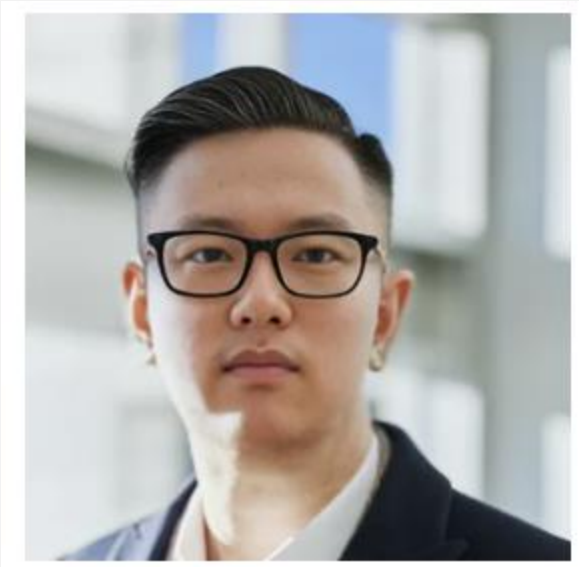
- Applied for Principal Software Engineer
- English-sound name
- Submitted resume (& picture after hired)
- Appeared to be a US-born citizen living in the US (of Asian descent)
- Claimed to be educated in Hong Kong
- Claimed to have worked at several well-known US companies
- Did 4 Zoom interviews
- Passed technical skills checks, reference checks, passed background checks

KnowBe4 North Korean Fake Employee



- Hired
- Shipped Apple laptop and FIDO-enabled Yubikey
- Employee asked for laptop to be shipped to new location
- July 15, 2024, at 9:55PM EST, “employee” powered on the laptop
- Tried (and failed multiple times) to install password-stealing malware
- 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
- Tried to manipulate session history logs

KnowBe4 North Korean Fake Employee



- EDR alerts were generated
- KnowBe4 InfoSec SOC staff alerted
- Reached out to employee on Slack to see what was going on
- Employee made weird excuse that they were troubleshooting speed issue on their router
- SOC member asked them to do an audio session to discuss more
- Employee refused
- Laptop isolated at 10:20PM, 25 min after first alert

KnowBe4 North Korean Fake Employee

- We shared the collected data with our friends at Mandiant, a leading global cybersecurity expert, and the FBI, to corroborate our initial findings
- North Korean fake employee identified
- Stu Sjouwerman (KnowBe4 CEO) notified
- Laptop returned when requested
- Stu tells staff about it in the daily meeting
- July 23,2024 - Releases public blog post
- Story goes viral

Stock photo NK used

AI-Photo Blending NK emp in

https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

KnowBe4 North Korean Fake Employee

- Lots of press coverage and media interviews
- Over a dozen other companies shared their own NK fake employee experiences with us
- Many other companies and law enforcement thanks us for sharing our experience publicly
- We created two webinars, a whitepaper, and multiple articles to cover and educate

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

North Korean Fake Employee Background/Ecosystem

KnowBe4

North Korean Background/Ecosystem

Overview

- Has been going on in some form for over a decade
- Used to focus on becoming freelancers and contractors
- Morphed to remote full-time employees during COVID with WFH jobs
- US gov't first warned about it in 2022, but focused on fake freelancers/contractors

May 16, 2022

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

The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) are issuing this advisory for the international community, the private sector, and the public to warn of attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to obtain employment while posing as non-North Korean nationals. There are reputational risks and the potential for legal consequences, including sanctions designation under U.S. and United Nations (UN) authorities, for individuals and entities engaged in or supporting DPRK IT worker-related activity and processing related financial transactions.

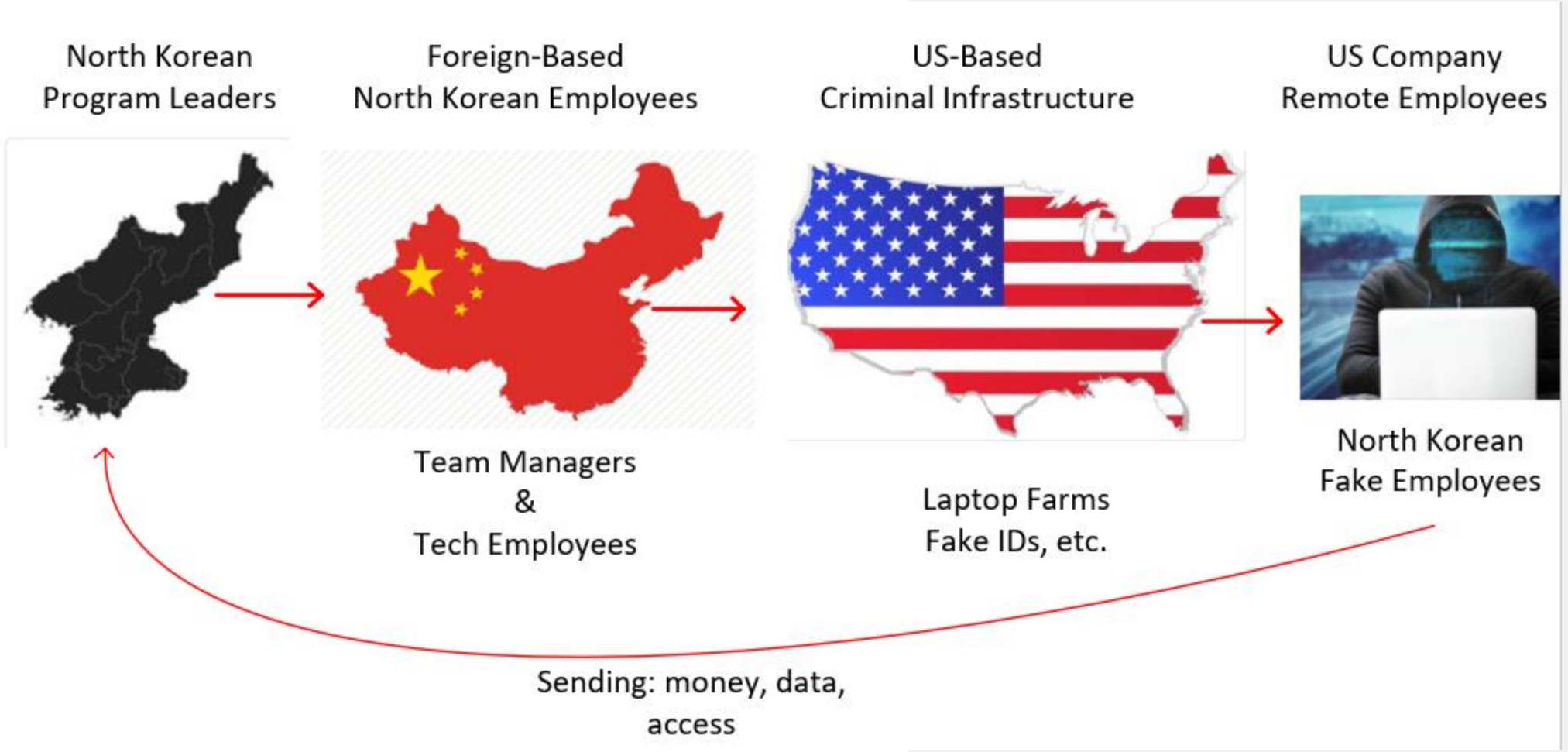
North Korean Background/Ecosystem

Overview

- North Korean fake employee program also known as Democratic People's Republic of Korea (DPRK) IT Workers program
- Officially supported by North Korea and DPRK leader Kim Jong Un
- Brings hundreds of millions to billions of dollars annually back to DPRK
- Created to circumvent US and UN sanctions that prevent hiring, working with, or sending money to North Korea
    - UN Security Council resolution 2375 (https://main.un.org/securitycouncil/en/s/res/2375-%282017%29)
    - US Dept of the Treasury's Office of Foreign Assets Control (OFAC) Economic Sanctions Enforcemer Guidelines, 31 C.F.R. part 501 and North Korea Sanctions Regulations, 31 C.F.R. part 510

North Korean Background/Ecosystem

Major Components



North Korean Background/Ecosystem

Major Components – NK Employees and Managers Based in Other Countries

- Usually China
- But can also be Malaysia, Europe, Russia, Africa, and other Asian countries
- Manager/Minder – manages team of employees
- Employees live together in close quarters
- Employees work together in call center-like area
- Employees only get to keep a small amount of the money they earn, manager skims some for self and operations
- 90% of earned money is sent back to North Korea

North Korean Background/Ecosystem

Major Components – Non- North Korean Scheme Assisters

- Laptop Farmers

Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator

According to court documents, Knoot ran a "laptop farm" at his Nashville residences between approximately July 2022 and August 2023. The victim companies shipped laptops addressed to "Andrew M." to Knoot's residences. Following receipt of the laptops, and without authorization, Knoot logged on to the laptops, downloaded and installed unauthorized remote desktop applications, and accessed the victim companies' networks, causing damage to the computers. The remote desktop applications enabled the North Korean IT workers to work from locations in China, while appearing to the victim companies that "Andrew M." was working from Knoot's residences in Nashville. For his participation in the scheme, Knoot was paid a monthly fee for his services by a foreign-based facilitator who went by the name Yang Di. A court-authorized search of Knoot's laptop farm was executed in early August 2023.

https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and

North Korean Background/Ecosystem

Major Components – Non- North Korean Scheme Assisters

- Laptop Farmers

Arizona woman charged in worker scheme that raised

By Sean Lyngaas, Holmes Lybrand and Evan Perez, CNN

4 minute read · Updated 3:50 PM EDT, Thu May 16, 2024

(CNN) — US federal prosecutors on Thursday charged an Arizona woman with participating in an elaborate fraud scheme to help foreign IT workers pose as Americans, get hired by major US companies and earn $6.8 million in revenue that could benefit the nuclear-armed North Korean regime.

The scheme compromised the identities of 60 Americans and affected 300 US companies, including a major national TV network, a "premier" Silicon Valley tech company, and an "iconic" American car maker, says an indictment unsealed in the US District Court for the District of Columbia. The indictment did not name of the companies.

The Arizona woman, Christina Chapman, is accused of running a "laptop farm" from her home, in which she logged into US company-issued laptops on behalf of the foreign IT workers to trick companies into believing the workers were living in the US. At least some of the workers are described as North Korean nationals in the indictment.

https://www.cnn.com/2024/05/16/politics/woman-charged-north-korean-it-worker-scheme/index.html

North Korean Background/Ecosystem

Major Components – Assisting Infrastructure

- Accepting payments and the remitting to NK
- Generating fake identities or stealing real identities
- Creating fake employee websites and projects
- Create fake IT companies
- Giving references
- Money laundering
- Document forgery services
- Websites, etc.

KnowBe4 North Korean Fake Employees

- Likely thousands of fake NK employees working for companies around the world
  - Fortune 500 companies, companies with 12 employees
  - Any remote-only position/contractor position at risk
- Likely many tens of thousands of job applicants are fake employees
- Don’t forget about fake companies, too

Signs of a North Korean Fake Employee

KnowBe4

Signs of a North Korean Fake Employee

Before Hiring

- Presents themselves as Asian (e.g., South Korean, Chinese, Malaysian, Japanese, etc.), European, or US-based
- Will often claim to have always lived in the US, gone to only US-based universities, and worked for well-known US-based companies, even though their English is limited
- Will often claim to be a US-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)

Signs of a North Korean Fake Employee

Before Hiring

- 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

Signs of a North Korean Fake Employee

Before Hiring

- 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 interview from a nosy (call center-like) background

Signs of a North Korean Fake Employee

Before Hiring

- 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 excuse for why camera isn't working

Signs of a North Korean Fake Employee

After Hiring

- Wants you to mail organization devices to additional location not indicated on employment application or previous communications
- You detect unnecessary remote login on the organization's device
- IP address where the organizational device is logging on from does not match claimed location
- You detect malware on the organizational device

- You detect unusual behavior or the organizational device
- Changes to log files or other cover-up attempts on the organizational device

Signs of a North Korean Fake Employee

After Hiring

- Work hours don't seem consistent with country or region being claimed, emails and work product seem to always 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've been detected and shutdown on the old email address)
- Inconsistent project delivery quality, definitely doesn't seem to meet quality of person interviewed

Signs of a North Korean Fake Employee

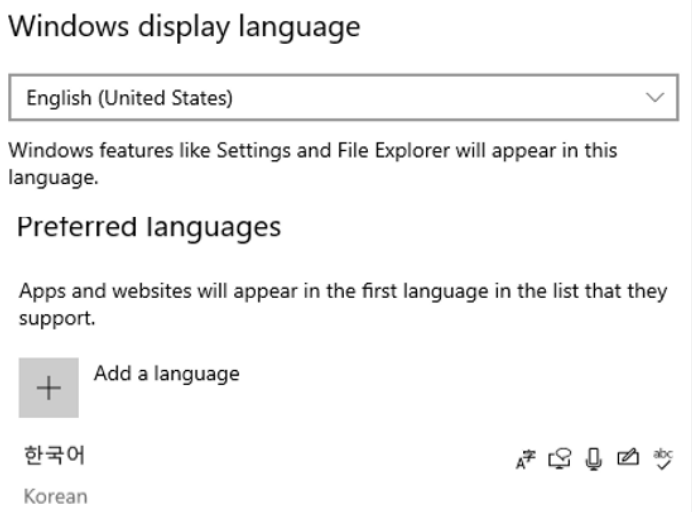
After Hiring

- 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 is sent to a bank, banking details provided for payment are to a unfamilar bank or don’t match public records
- They request that payments be made to virtual currency, cryptocurrency, or other popular money exchange sites (e.g., PayPal, Venmo, etc.)

Signs of a North Korean Fake Employee

After Hiring

- Employee changes OS or application to Korean language support even though the claim to be of another nationality



Note: Employee/candidate doesn't have to meet all criteria, just a few of these should raise suspicions

How to Defend

How to Defend

Before 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 don’t have an existing fake employee

How to Defend

During Hiring Process

- If possible, always require that remote employee to physically meet with a trusted employee, team leader, or selected agent of the organization in person, with an official ID, to confirm they are who they say they are

How to Defend

During Hiring Process

Recruiters

- Recruiters are getting besieged by North Korean fake employees
- Most are aware of the problem and look out for suspicious signs
- But many employers who have hired North Korean fake employees did so because they were brought to them by a trusted recruiter
- Make sure your recruiter is educated about the problem

How to Defend

During Hiring Process

- 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

How to Defend

During Hiring Process

- If possible and reasonable, and if the employee candidate has 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 candidate and references
- Check references
- Require that all professional/work references be made to legitimate and publicly confirmable business phone numbers and email addresses (don’t allow generic public email addresses only)

How to Defend

During Hiring Process

- Use a background check that looks for fake employees
- Require that candidate use 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 remote candidate to submit fingerprints for identity verification purposes

How to Defend

During Hiring Process

- Review lists of known North Korean fake employees

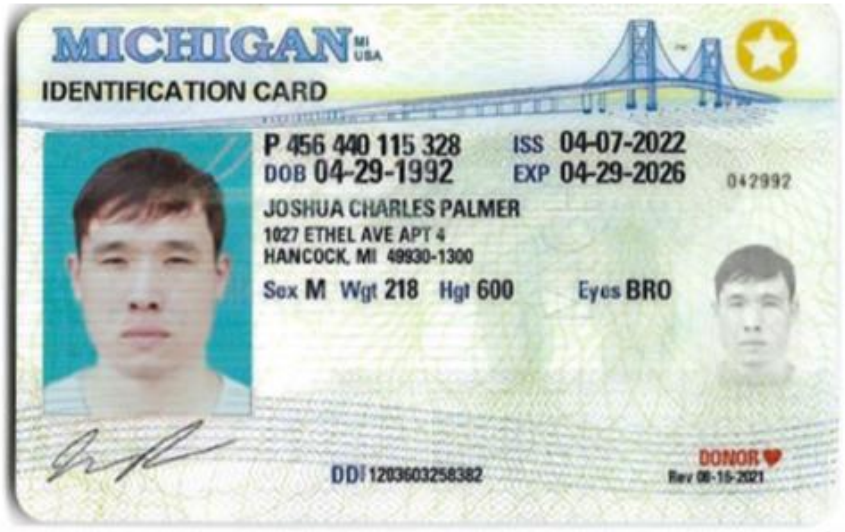
Fake Name	Payment address	Fake Location	Github	Email
Jason Kwon	0x4b94ba1528636a699dab486a217d39bb7ce21d75 0x1075e62bfacbb44e31d7a5719e55c7d16fe7d35d 0x7969b188f7dc6bf80d68f224ac3454dafe6f6d5d 0xa771609C5C56048f146d2C794c87DB946bfF27Cf 0x90cf352dDAF171d41A6DEd1d54cEDA4005047c93 0x72c70980ACddE7a5C9437050E73E7d07fBf21D25	Canada	https://archive.ph/J347l https://archive.ph/Wlu3i	0xm00neth@gmail.com
Willie Lee	0x97e36fAE76cD7ef7cC1213927A9A4E10a61CdD8d	California, US	https://archive.ph/SjJfK	willie.lee226@gmail.com
Naoki Murano	0x6188a9e76794e7cb337b8E5a2B91808Ce34Fc6D1 0x85e0504fcd7981baa68774431099c5e2dcf074dd	Tokyo, Japan	https://archive.ph/96QVA	naokimurano@outlook.com
Sano	0xef2a0324cfaa0100db9def8ef31c6e23bc4f9258	-	https://archive.ph/KMoXG	-
Jun Kai	0x8aa07899eb940f40e514b8effdb3b6af5d1cf7bb	Singapore	https://github.com/junkai121	junkai121@outlook.com
Kei Nakano	0xff22be4f00b937dade564bd9659e265f92afa620 0x452f205c6c3872691fbce7ce8438370466d55f76 0x21e5d5a6e40b32cff77cfe77dca034d6d410131d	Tokyo, Japan	https://archive.ph/mo0QZ https://archive.ph/fhKTT	keinakano415@gmail.com
David Adachi	0x210888f2624d01f9cbc71de5bf4caf5b6dc9fa7f	Fukuoka, Japan	https://archive.ph/80EYH	davidadachi56@gmail.com
Gabriel Yiu	0xd80614feb54d49cf46cc861fc549fae0a05b3f7e	-	https://archive.ph/oGlCc	-
Joshua Palmer	0x06f90983cd2215379e440fc525e441d6a5fc3fba 5Jfb3n8eW4JyQrKJktMNBFXnC1zx2YHjRSkzRrTT5QHh 0xa6afe0290fb6f2f7ced0a2753de57f9fa7c9c9dd 0xfa802d9b33ed74baff62b189875c2b2d192874eb 0x7654e18ff3495675606c008a39b6264da5d0e8a7	Michigan, US	https://github.com/call-by https://archive.ph/grqjk	joshupgig@gmail.com smart.solidity@gmail.com
Andy Hoog	0x1043efee936903951b88db23551873bb67292e95	-	https://archive.ph/7IbnH	andyhoogup@gmail.com
Jordan Lopez	0x92cd7363c5b1853bc8fe6b5ae269836fc508ca73	Texas, US	https://archive.ph/tFeQG	cloudrider.m92@gmail.com
Quinn Lee	0x9de5d3158b0b83e9211c7444c94ce0c53763f574 0xf9adac8658e08893fb4e91c1062e471eb11cb6c7	-	https://archive.ph/KLBYw	letteldream@gmail.com
Ryuhei "Rio" Matsuda	0xa71b641a498e33bb13548a01eca5e20e083e637b 0x6fb678b2dd9d2ff50ee9ecf774251dcceb7a2da8	-	https://archive.ph/V5GsZ	ryuheimat3@gmail.com
Chris Yu	ESSfP3aAcW6Z59ozut9Jkqy9btaX5YTHt25b3Vhs2hsf 0x1043efee936903951b88db23551873bb67292e95 0x3b9A870c24905256dE10863cb360F4B93C7cC60f 0xc2b2a9c05740EEb7ee7BA7eB3AB11EC8bebCB1D1	Malaysia	https://archive.ph/x0LMf	atroboj@gmail.com

https://github.com/shortdoom/gh-fake-analyzer/blob/main/profiles/INVESTIGATIONS/ZachXBT_15.08.2024/Attackers.jpeg

How to Defend

During Hiring Process

- Review lists of known North Korean fake employees



Fake Name	Payment address	Fake Location	Github	Email
Ryunel "Rio" Matsuda	0x6fb678b2dd9d2ff50ee9ecf774251dcceb7a2da8	-	https://archive.ph/v5GsZ	ryunelmat3@gmail.com
Chris Yu	ESSfP3aAcW6Z59ozut9Jkqy9btaX5YTHt25b3Vhs2hsf 0x1043efee936903951b88db23551873bb67292e95 0x3b9A870c24905256dE10863cb360F4B93C7cC60f 0xc2b2a9c05740EEb7ee7BA7eB3AB11EC8bebCB1D1	Malaysia	https://archive.ph/x0LMf	atroboj@gmail.com

https://x.com/zachxbt/status/1824047425822310580/photo/2

How to Defend

During Hiring Process

- Use Open Source Intelligence (OSInt) Tools

Malicious Github Accounts

DISCLAIMER: The confidence in detecting "malicious" GitHub profiles is low. Many regular user accounts may appear in the analysis files; this does not indicate their participation in any illegal activity. ANYBODY can edit the `.git` file, and ANYBODY can commit code to GitHub. This tool is intended for reconnaissance purposes only.

It's possible, to a certain degree, to define some metrics for classifying GitHub profiles as potentially malicious. However, motivated enough attackers can still bypass most of those checks and appear as professional engineers. If that's the case, a company should fall back to regular methods of judging a potential employee/contact. The following script can help out with finding some dark patterns if the attacker is not motivated enough :)

1. Does any (not forked) repository or commit predate the account creation date? If yes - suspicious.
2. Does any (not forked) repository have more contributors than the owner? If yes - check contributors; it can be suspicious on small accounts.
3. How many unique emails do you find in commit messages? If many - suspicious; account used on many different PCs with many different credentials.
4. Does any commit message appear copied from another repository? If yes - suspicious; owner probably copied the original repository and edited .git history.
5. While getting "all repositories" for an onwer account, do some repositories return an error with DMCA takedown? If yes, suspicious.

Great list of flags by ZachXBT: https://x.com/zachxbt/status/1824047480121729425

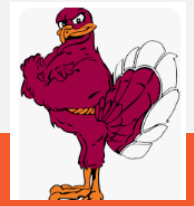
https://github.com/shortdoom/gh-fake-analyzer/tree/main#malicious-github-accounts

How to Defend

During Hiring Process - Optional

This last suggestion isn't 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?"



How to Defend

During Hiring Process – Optional – Example Questions

- 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?”

How to Defend

During Hiring Process – Optional – Example Questions

- “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?”
- “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?”

How to Defend

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 logons
- 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

How to Defend

After Hiring

- Monitor activity against purported normal work hours
- Require employee be on camera during training or anytime when communicating with another employee
- Randomly ask 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.

More to Read

Other Sources – US Government (FBI, DOJ, Treasury)

- 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)
- 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

More to Read/Watch

KnowBe4 Resources

KnowBe4 has many articles, two webinars, and a whitepaper on this subject

- Articles (https://blog.knowbe4.com/)
- Webinars (https://www.knowbe4.com/webinar-library)
- Whitepapers (https://www.knowbe4.com/whitepapers-and-ebooks)

- Just search on ‘North Korean’

More to Read

Other Sources – KnowBe4, Mandiant, WSJ, Others

- https://blog.knowbe4.com/north-korean-operatives-infiltrate-job-platforms
- https://www.nisos.com/research/dprk-it-worker-scam/
- Mandiant Principal Analyst, Michael Barnhart, joined The Defender's Advantage podcast (https://open.spotify.com/episode/0xeaavXjlX2XLm3oibOv6g
- https://www.wsj.com/politics/national-security/american-it-scammer-helped-north-korea-fund-nuclear-weapons-program-u-s-says-65430aa7
- https://www.wsj.com/articles/deepfakes-fraudsters-and-hackers-are-coming-for-cybersecurity-jobs-e2a76d06

Platform for Awareness Training and Testing

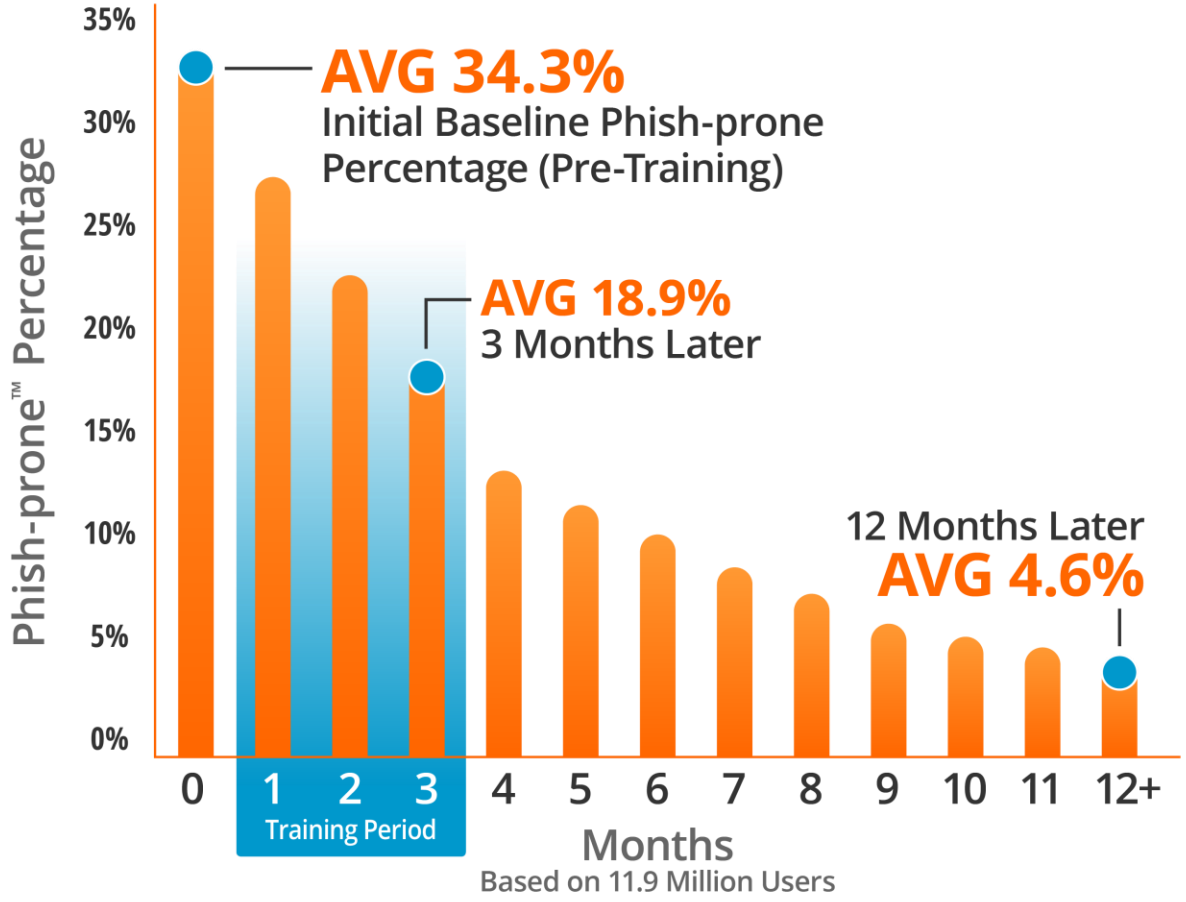
1. **Train Your Users**
2. **Phish Your Users**
3. **See the Results**

Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

86% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2024 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
e: rogerg@knowbe4.com
LinkedIn: https://www.linkedin.com/in/rogeragrimes/
Mastodon: https://infosec.exchange/@rogeragrimes
Twitter: @RogerAGrimes