vb 2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

ROGUE HIRER, ROGUE HIREE: WORKPLACE CYBER THREATS TO INDIVIDUALS AND BUSINESSES

Chris Boyd

Rapid7, UK

ABSTRACT

In a volatile job market, fraudsters and threat actors are causing misery, data loss, and financial harm for employers and employees alike.

While DPRK threat actors [1] use elaborate laptop farms and stolen identities to work their way inside organizations, individual applicants exploit gaps in the hiring process to make their way from shortlisting to onboarding. Meanwhile, unwary job applicants are forced to run a gauntlet of fake companies, tax fraud, money muling and data harvesting while looking for genuine employment.

This research zeroes in on business-centric threats, exploring the most common archetypes of rogue hires. We explain what attackers want, how they intend to get it, and the tactics used to make a beeline for your organization's most valuable assets. We provide actionable guidance for securing the riskiest stages of hiring, and how you can channel adversaries toward total process failure.

Readers will gain insight into the kind of attacks an organization needs to defend against, and a list of questions they can take back to base to ask, 'Do we have a plan for this?'.

The paper expands on these questions, covering business-centric threats and also the many risks that face individual job applicants.

From *LinkedIn* to dedicated hiring portals, the potential for falling into a fake job trap and get-rich-quick schemes is high. Malicious files hidden in coding tests, compromised *LinkedIn* pages promoting money muling, and spam mails arising from genuine job portal applications will all be highlighted and countered with common-sense solutions.

Both paper and presentation aim to highlight the most significant hazards facing the workplace, or emanating from it, and give attendees practical steps to reduce the risk arising from malware attacks, data exfiltration, and sending funds to sanctioned regimes. Your hiring activities and digital defences will ultimately become more robust, no matter which side of the hiring table you sit at.

INTRODUCTION

New entrants to the job market face significant barriers to success in the hiring process. In the latter half of 2024, several studies indicated that a sizable portion [2] of job adverts are in fact 'ghost jobs' – fake listings intended to maintain a company presence on hiring boards, or simply harvest applicant resumes at scale. One survey highlighted that 81% of recruiters [3] admitted to posting fake company openings, with 38% wanting to maintain a job board presence even when not hiring and 12% simply wanting to collect resume data. Another survey found that three in 10 companies listed vacancies that were not real [4], often for similar reasons including resume harvesting and presenting the appearance of growth.

Worse still, many job opportunities are outright fraudulent – bogus offers, wire fraud, savings theft and more besides are all waiting in the wings. For example, in 2022, the FTC reported a $367m loss [5] impacting American consumers to job scams, involving everything from check fraud to gift card offers – a 76% year-over-year increase. In 2023, the Identity Theft Resource Center stated that reports of recruitment fraud – primarily 'carried out through websites, typically *LinkedIn* or job search platforms' – increased by 118% [6]. In the UK, Action Fraud received almost 5,000 reports of job fraud in 2024, compared to a little over 2,000 in 2022. Job seekers fell victim to an assortment of fraud including fake training courses, bogus recruiter scams, and fictitious job opportunities, with an average amount lost per report of £4,707.

Meanwhile, businesses looking for genuine employees are faced with a rise in AI-generated resumes [7], applicants who may have malicious intentions, and rogue hires [8] from nation states intent on directing funds to activities such as ballistic missile development. More than ever, it's become essential to map out strategies for dealing with nation-state attackers, so-called proxy employees, and people intent on damaging a business either through malware deployment or data exfiltration.

DANGERS TO BUSINESSES

A wealth of threats lie in wait for unwary businesses, and the sections that follow cover a variety of topics that your organization should consider when drawing up a secure hiring process, from real-world security to popular tactics deployed during and after the hiring process.

North Korean IT workers

The problem of fake IT workers from North Korea embedding themselves in businesses around the world is now a firmly established cyber threat [9], not to be taken lightly. Rogue hires are so common that individuals in the US will not only help

to validate stolen identity documents [10], but also play host to laptop farms [11] in order to make fake worker locations appear to be genuine.

Given that businesses also hire freelancers and contractors alongside full-time employees, it is alarmingly easy to gain a temporary foothold into a company and cause no end of reputational or financial damage.

Worse still for security teams, there's no way to know in advance if a rogue hire is there to do damage and exfiltrate data, or instead function as a regular employee and send money back to North Korea at the end of each month. Whether your business lives or dies by the rogue employee sword is almost entirely a matter for the hiring process.

Hidden from view: DPRK laptop farms

Things become even more complicated considering that DPRK is doing a little side-gig recruitment of its own. North Korean rogue hires are scoring wins as a result of laptop farms popping up across the target nations [12] where the fake hires claim to reside.

The growing number of farms coming to light in the press are based in the US, operated by American citizens managing remotely operated corporate laptops intended for the North Korean employees.

How does this work in practice? Fake applicants apply for positions with a US address tied to the stolen identity being used for the interview and background checks. Once hired, the North Korean worker informs the business that they're moving address and asks for the company laptop to be sent to the new address: the laptop farm.

Take the case of Christina Chapman [13], who was offered a position on *LinkedIn* as the 'US face' of a company generating jobs for overseas IT workers. As the *The Wall Street Journal* notes [14], there is no indication she had any awareness of having involvement with North Korea. Even so, she pleaded guilty [15] to 'conspiracy to commit wire fraud, aggravated identity theft, and conspiracy to launder monetary instruments'.

Here, as with unknowingly becoming a money mule, not understanding what you've got yourself into is potentially no defence whatsoever in the eyes of the law. And this is 'just' the person operating the laptop farm. Businesses finding themselves inadvertently funnelling cash to North Korea may fall foul of legal complications [16] due to violation of sanctions.

Malicious applicants

Malicious applicants – people working alone or in small groups to gain employment with the intention of harming their new employer in some way – are not a threat to be taken lightly. While they are perhaps not quite as panic-inducing a problem as DPRK running amok inside your server farm, you simply cannot predict what the end-goal is. Maybe they simply want to do the bare minimum and coast by, picking up paycheck after paycheck. Perhaps they intend to pay someone to act as a proxy worker while they put their feet up and generate money for nothing. Or maybe they intend to gain trust over time, eventually being granted access to sensitive business material. At this point, they could sell the data to a business rival or simply offload everything into the dark web.

With the worry of figuring out the initial access vector removed from their infiltration plans, they're free to map out phishing attacks against co-workers, or try and sneak an infected spreadsheet to somebody in finance. With enough intel on the inner workings of the business and a handy structure map plucked from *Zoom* or internal help pages, they may even decide to indulge in a business email compromise (BEC) attack.

Infostealers in the workplace

Thanks to an array of DIY kits and malware-as-a-service (MaaS), it's never been easier to get your hands on the rogue file you need to get the job done. If an attacker is feeling particularly determined but doesn't want to do all of the work, then there's a variety of initial access broker forums able to assist for the right price.

If someone is already happy to jump through recruitment hoops to steal data or do damage, one has to assume that they're already fully aware such services exist and would consider using them to achieve their goal. *Rapid7*'s own Q1 2025 incident response data [17] highlights that infostealers with a low barrier to entry are some of the most popular infections post initial access that we consistently observe.

A few hundred dollars gets a would-be attacker lifetime access to BunnyLoader, and a wealth of features that include keylogging and clipboard / credential theft. 40% of all cases observed by *Rapid7* from January to March of 2025 involved BunnyLoader, leading other malware by a considerable margin across 12 of 13 industries overall and dominating across manufacturing, comms, healthcare, and business services. Figure 1 illustrates the prevalence of incidents observed involving BunnyLoader payloads across the top 5 industries.

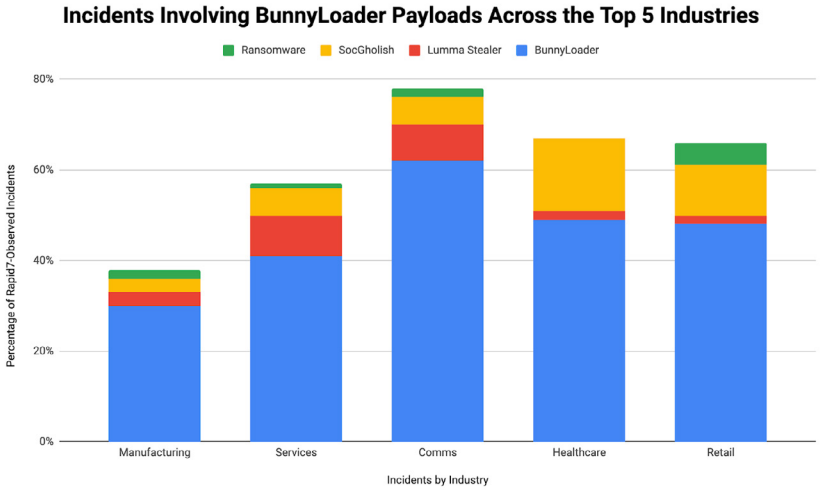


Figure 1: Incidents involving BunnyLoader payloads across the top 5 industries.

If it's so easy to deploy from outside the network, imagine how much power a would-be attacker possesses with full permission to live inside the corporate ringfence.

And finally... don't forget about physical security

Physical security is also an issue that can put digital data at risk. Plenty of potentially valuable items (or even pieces of information) are left out in the open in many offices. Everything from watermarked paper to passwords on Post-it notes are fair game when a rogue is on the loose. *Rapid7*'s pen testing assignments to test the building security of other businesses during open interview sessions have revealed candidates left alone to explore the office unhindered, figure out technology stacks and potentially vulnerable endpoint software, and observe unattended and logged in devices.

THE THREE STAGES OF HIRING: WEAK SPOTS

During the interview process, rogue applicants are trying to bypass any security measures in place for screening and interviews. They also know that if they make it past the first two stages and are hired, realistically whatever checks are in place for onboarding are mainly looking at performance as opposed to weeding out fraudsters.

Screening and shortlisting

An authoritative-looking resume and a sheen of credibility on work history is intended to dampen the desire for in-depth investigation. Here's what you can do at this first hurdle to weed out a scammer:

- Background checks and applicant tracking systems (ATS): There are now lists of email addresses associated with a variety of cybercrime, including North Korean IT workers [18]. These systems are ideal for quickly making associations between potentially dubious data or even emails being reused across multiple applications to your business. On a similar note, background check services can cross reference with fraud databases, or even verify the legitimacy of a university degree or course transcripts alongside biometric data.

  This is particularly important in a world where fake experience letter [19] services exist. These services offer everything from fake wage slips to job credentials, along with a detailed list of bogus experience for submission to employers. Some will tailor their output to the specific job being applied for. As a typical example, one service located in India charged roughly $80 for a letter detailing six months of faked work experience. Their top level of service resulted in fakes listing up to three years of experience for around $230.

- Digital realness: If the applicant has a *LinkedIn* profile, it's worth spending time exploring the reality you've been presented with. Does the profile picture look like a stock photograph, or suspiciously AI generated? Does the individual have no contacts in your industry, yet claim to have worked in it for a long time? Is the profile relatively new? Do any of the dates provided contain chronological errors? Are recommendations entirely absent? One or two of these may signify an issue. The presence of many or all of them should definitely give you pause for thought.

Interview

This is where the desire to be as evasive as possible can massively help – or seriously hinder – the rogue hire. They'll want to conceal location, or lack of knowledge, or even their real face during the interview process. Here's what you need to do:

- Rule maker, not rule taker: You're in control of your own interview process. Insist on some easy-to-follow rules prior to the call(s). An initial conversation by landline or mobile can help establish the candidate's actual location. Request that blurred backgrounds be turned off for video calls, and that any earpieces (which can be used to feed the candidate answers) be removed.
- No AI, please: Fake workers abusing AI overlays to conceal their identity is part and parcel of the fake hire threat. While they can be convincing, they're not perfect. Look out for visual oddities tied to eye movement and lip-syncing. If in doubt, ask the candidate to pass their hand across their face as this will disrupt or break the AI generated overlay.
- A DIY personality test: Ask a few questions about personal details on the resume, such as hobbies or favourite sport teams. Casually quiz them on aspects of the city they live in. If the answers begin to dry up, you may have caught a rogue hire in the act. If you have more than one interview, track the consistency of answers across each session as this can be another indication of somebody making it up as they go.

Onboarding

If the rogue hire has made it this far, you still have options.

It may be prudent to restrict access to sensitive data or the ability to upload files to your systems. If they only need to upload old payslips or tax details to your system in the first two weeks, why hand over the keys to the kingdom? Restricting access to *Microsoft Teams* and *Slack* channels can also help here.

On a similar note, new remote hires should not be able to install remote management tools (or indeed anything else) without having to request it directly from the admin team. Any form of attempted tampering should be detected and reported by security software. When possible, an equipment collection or delivery should require the presentation of valid identification documentation, which may help reduce the risk of delivery to a laptop farm.

DANGERS TO HIREES

Targeting individuals is an attractive proposition for criminals; people outside of traditional business structures have little support or large legal resources to fall back on when things go wrong.

Below, I list some of the most popular forms of attack currently targeting people working for themselves, alongside a few notes of caution when applying for positions generally.

Job site spam (accidental or otherwise)

Job sites are all about openly sharing otherwise sensitive information with complete strangers. Would you post your mobile number or home address to social media portals? No, you wouldn't. However, a typical profile and resume may contain everything from home address to private mobile number, email addresses, and more besides. The more open you make your profile to potential employers, the easier it is for spammers and scammers to harvest your data or approach you with fake job offers.

Many job postings may require data to be filled in outside of the initial hiring portal, which itself comes with additional data collection requirements that the applicant may not be aware of. Family members have told me about filling in pop-up windows during applications which they assumed to be part of the job site, but were actually unrelated portals signing them up to additional hiring lists. Here are some things you can do to reduce the likelihood of this happening to you:

- Make use of disposable email addresses, ideally one per job site. If your data is leaked or used for additional sign-ups, you'll know where it came from.
- Some job sites use additional privacy features to address these problems. *Indeed*, for example, shields the applicant's email address [20] when interacting with employers.
- Application processes making use of AI research [21] or third-party multiple choice assessments [22] will almost certainly use your data in ways you may not have envisaged.
- Reduce and remove data from your resume. Email, date of birth, full address, payment details, and phone number should never be included. Some sites allow you to have a condensed public version and a full version specifically for employers.
- Always keep track of where you've uploaded your resume, which version, and how to deactivate your account once you no longer need it. The job site *Reed* allows you to 'pause' your account, which means recruiters can't view it [23] until you amend your contact preferences.

Task scams

Task scams sprang to prominence at the end of 2024 [24], where the promise of big earnings working from home ensured a steady drip-feed of victims. The scam operates like this: fake employers target gig-economy workers with gamified 'tasks',

which promise a cut of money for every group of tasks completed. The more tasks they complete, the more they level up and the more money they can earn.

The scam is successful because the fake employer sends a small outlay of money to the victim, making them believe that their job is legitimate. The target is asked to perform repetitive tasks – such as posting fake reviews for hotels they've never visited, or spamming movie promotions – and 'unlocking' the next level of rewards for a job well done.

There may also be additional financial rewards for 'checking in' every day. Initially, the gig-worker does receive regular small sums of money to keep up the appearance of actual paid work. However, as the higher tiers unlock, the worker is asked to pay large sums of money back to the fictitious company that they're supposedly working for.

Multiple high-value tasks will be given to the worker simultaneously, with earnings supposedly subject to various forms of income tax. This 'tax' needs to be paid to release the earnings – which, of course, will never happen. Depending on the task website's ToS, it could be anything from a 40% tax on amounts over $12,000 to 35% on totals over $30,000. Either way, the amount referenced will not be pocket change.

Even if you're not looking for work, you may be contacted out of the blue on services like *Telegram*, like I was in the example below:

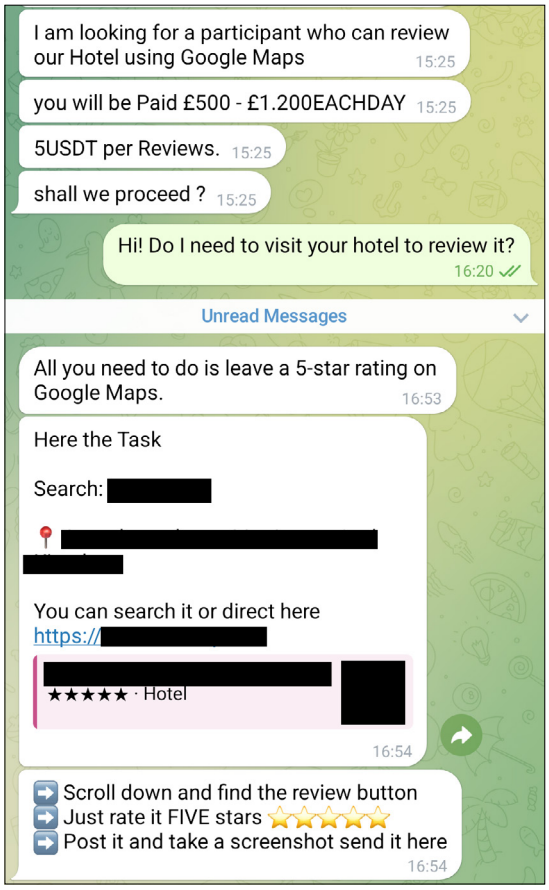


Figure 2: Messaging spam asking me to rate hotels.

By the time the victim realizes that their early payouts have been replaced by a fake tax payment hole where their savings once resided, it's often too late to do anything about it.

When attacks branch out

Within a few days of complaints raised about certain task sites on *Reddit*, recovery service providers were already mentioning them in hashtag form on sites such as *Instagram*. Many of these accounts claim to be 'ethical hackers' or black hats able to recover stolen funds for a fee. The problem here is that there is no guarantee that paying for such a service will do anything other than subject the victim to a refund and recovery scam [25].

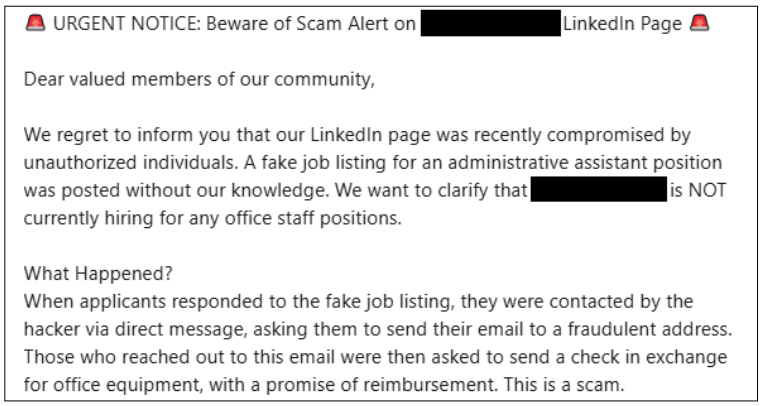
Are these recovery accounts monitoring scam assistance subreddits [26], and making a note of the scam portals mentioned? If they are, it would be an easy way to rise to the top of search results for popular, active scams. It's also possible that the people behind the task scam set up fake recovery services themselves to try and double-dip the victims.

Common indicators of danger, and what to avoid:

- Task sites often abuse the branding of major legitimate services. Contact the service via official channels to determine if what you've been sent is a scam.
- Payment progression which has been overly gamified, or represented as a series of video game unlocks, is a very common sign of a task scam.
- Ambiguous references to unspecified tax laws, which claim the employee needs to cover the cost of any amount beyond a certain percentage, should be viewed with suspicion. This is listed largely to trigger the final stage of the scam, where large payments are sent by the victim.

LinkedIn compromises

An individual's insecure *LinkedIn* profile is a gateway to social engineering attempts on contacts, work colleagues, and members of the public. If an attacker hijacks a business profile, the reputational and financial harm to an organization could be devastating. At the bare minimum it will require an explanation post, such as the one below where a business account was compromised and used to post a fake job listing. Applicants were contacted via direct message, and asked to send on money in return for office equipment.


🚨 URGENT NOTICE: Beware of Scam Alert on [redacted] LinkedIn Page 🚨

Dear valued members of our community,

We regret to inform you that our LinkedIn page was recently compromised by unauthorized individuals. A fake job listing for an administrative assistant position was posted without our knowledge. We want to clarify that [redacted] is NOT currently hiring for any office staff positions.

What Happened?
When applicants responded to the fake job listing, they were contacted by the hacker via direct message, asking them to send their email to a fraudulent address. Those who reached out to this email were then asked to send a check in exchange for office equipment, with a promise of reimbursement. This is a scam.

Figure 3: A warning about a compromised account posted to LinkedIn.

This is a classic case of check fraud. Once the victim sends money to what they believe to be the office suppliers, the check bounces, with the funds sent making its way to the fictitious employers.

It could also be the first stage of a money mule scam, where the fraudsters ask the victim to both receive *and* send money for the supplies. The end result would be that the victim has passed stolen money through their account, and potentially made it harder for authorities to trace it.

Locking down your LinkedIn profile:

- Secure a unique password with an authenticator app, and consider protecting your password with a password manager. Valid accounts with no multi-factor authentication (MFA) enabled continue to be a big problem [17] where initial access is concerned.
- Get into the habit of checking the 'signed-in locations' list and 'devices that remember your password' in the 'account access' settings.
- Consider tweaking 'profile visibility', which you can use to restrict people viewing your connections, discovering you via email address / phone number, or view who you follow.

Fake coding tests

A threat aimed at gig-economy workers and freelancers generally, rogue code challenges are a popular way for individuals or nation states to infect systems [27].

Remote work has solidified remote coding challenges as an acceptable form of skillset challenge for applicants. Where this goes wrong is directing said applicants to code repositories where rogue code lies in wait.

Our research led me to an individual on *LinkedIn* offering coding challenges for cryptocurrency-centric positions. The account, using what is almost certainly a deepfaked image for a profile picture, claimed to be located in the Philippines and responsible for fintech and trading. Over a period of a week or so while I claimed to be seeking work, I was asked to take part in a coding challenge.

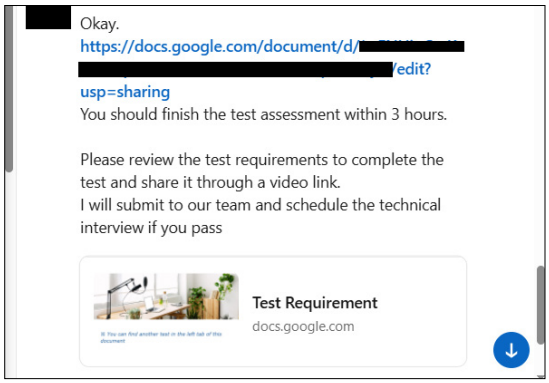


Figure 4: A link to a coding test.

Monthly salaries ranged from $6,000 to $15,000, with the hiring process consisting of four stages. A *Google Docs* link directed me to a code repository, which followed a pattern similar to that seen in the wild [28] on a regular basis [29]: the presence of the eval() function [30] in the repository as a likely means of executing malicious code [31].

Many of these attacks focus on developers involved in cryptocurrency [32], and there is, of course, a connection to North Korea [33] with this set of techniques too.

Interestingly, revisiting the hiring account revealed that it is now deleted on *LinkedIn*, and its messages are tagged by the platform as potentially harmful. The most likely result here is that a new fake profile will activate and point to a new collection of code.

Common indicators of danger, and what to avoid:

- Coding challenges offered on *LinkedIn* should be treated with suspicion, especially if you're not familiar with the recruiter.
- Multiple code challenges linked from a *Google* doc, even for positions that wouldn't typically require a coding challenge (e.g. graphic designer), may be suspicious – especially if each link leads to the same coding test.
- Many of these attacks begin with a claim that the recruiter's company is a division or affiliate of a major brand, despite no obvious connection to the legitimate business.
- Be wary of inauthentic *LinkedIn* profiles. Following lots of accounts but with no connections, incomplete sections, not tagged as working for a verified organization, and duplicate accounts may all point to a fictitious profile.
- Be mindful of potentially dangerous elements in the code which could lead to compromise. Do not run someone else's code in an unprotected, bare-metal environment.

Fake music industry offers

Artists and musicians are favoured targets for work-related scams, as the cost of materials and equipment is significant; any promise of money or a breakthrough deal is going to sound attractive to potential victims. One of the most common attacks involves fake artist and repertoire (A&R) agents approaching musicians on social media with the promise of fame and riches.

Social engineers will frequently imitate genuine music industry workers with details and photographs stolen from *LinkedIn* and elsewhere. The objective is to steer the musician away from the relative safety of their music platform, and onto messaging apps such as *WhatsApp* and *Telegram*. There, they'll converse with someone claiming to be the CEO of a music label. *Warner*, *InterScope Records* and *Sony* [34] are often used as bait to make the offers sound particularly attractive. If the music platform has a social component, such as *BandLab* and *SoundCloud*, then it's relatively straightforward to set up a fake account and message the intended victim [35].

Figure 5: A Reddit post regarding a fake Sony message.

These offers routinely lean into fake recording contracts, bogus video soundtrack offers, and more general promotional activities. If the people behind these scams designate you to be a particularly appealing target, you may receive a mixture of bogus offers:

Figure 6: A question about fake music industry messages.

In the example shown in Figure 7, I was quickly moved from the fake A&R representative to someone claiming to be Robert Stringer, CEO of *Sony Music Entertainment*. The offer? A signing bonus of $200,000 (which randomly changed between messages) and an 'average annual salary ranging from $200,000 with a median of $150,178'.

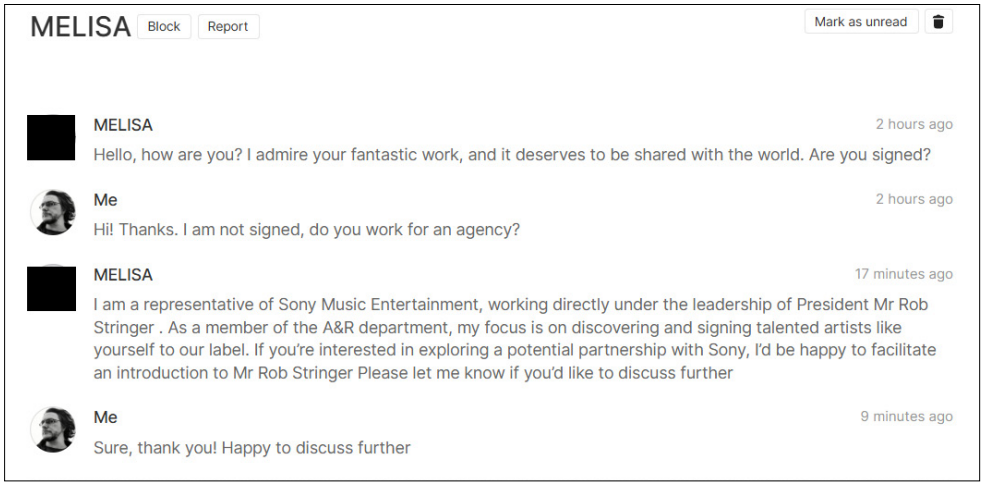


Figure 7: Fake music industry messages sent via SoundCloud.

These attacks are designed to end in one of several ways:

- Malware deployment / remote management tool
- Wire fraud
- Bogus purchases / cryptocurrency scams

In this case, the contract claimed I would need to pay $300 to purchase an unnamed project tracking tool, with the payment made via cryptocurrency or *PayPal*.

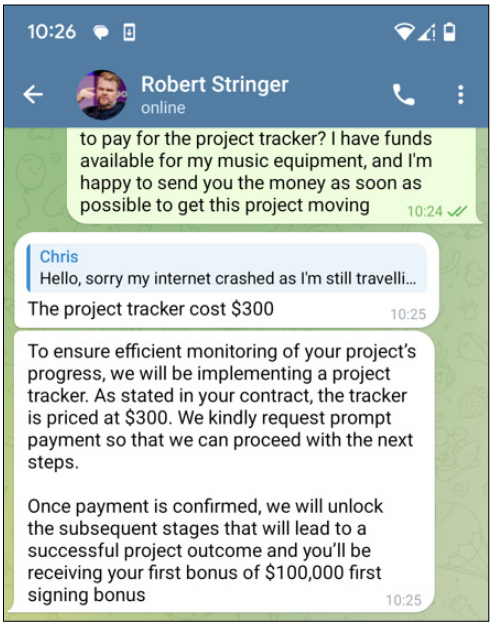


Figure 8: Messages regarding a fake project tracker.

The attacker was reluctant to share payment information, possibly because they wanted to ensure I was a genuine target before investing additional time in the attempt. Eventually, after several days of conversation, I was sent a *PayPal* address with a 30-minute timeout, and a Bitcoin address.

Figure 9: The scammer sending me a Bitcoin address

In total, the Bitcoin address given to me had received and sent a little under $6,000 between January and March of 2025 across 86 transactions. Inbound payments to the initial Bitcoin address ceased the same day as our final conversation. Most likely, the person or group behind it burnt the address after I failed to pay.

Common indicators of danger, and what to avoid:

- Beware of supposed A&R representatives of major music labels reaching out on music platforms including a social media component.
- Being connected with CEOs and heads of industry labels via messaging services such as *Telegram* or *WhatsApp* is extremely unlikely. The CEO of *Sony Music Entertainment* is not asking musicians to send him Ethereum.
- Contracts that ask the musician to pay for project tracking / management software, the hosting of an artist's web page, or to invest in promotional funding are not genuine.
- Deny requests to install remote management software, either on a PC or a mobile device.
- Don't be pressured into making a time-sensitive payment, especially via temporary *PayPal* addresses or cryptocurrency.

CONCLUSION

The problem of rogue hires has exploded in terms of media attention, with the realization that nation-state attacks are perhaps not the very unique boogeyman that they once were. While extremely targeted malware campaigns with a handful of victims in mind will never go away, there is a growing sense that broad rogue hire campaigns could actually happen to any unfortunate organization. Outside of DPRK-centric attacks, there will also always be small groups and individuals ready and willing to sow chaos inside a businesses' walls.

Similarly, the gig-economy is here to stay, alongside aggressive hiring cycles and layoffs, which may well increase the necessity of people going freelance. Some aspects of hiring expectations are snagged on rough edges that have no easy resolution. For example, people are encouraged to use business profile photograph sites to generate professional-looking headshots for applications. At the same time, ATS systems and hiring managers are increasingly screening out applicants making use of AI for both text and visuals. All of this is taking place under the hood while organizations deploying AI

detection systems have to worry about false positives and other edge-cases which may unfairly impact would-be employees.

While people's finances are stretched, they will continue to apply to 'too good to be true' employment opportunities and incur both monetary and data losses. By the same token, those with their sights firmly set on businesses will continue to make the most of remote opportunities courtesy of insecure hiring processes and a web of laptop hubs operating out of target nations.

REFERENCES

[1] Collier, J.; Barnhart, M. The ultimate insider threat: North Korean IT workers. Google Cloud. 6 March 2025. https://cloud.google.com/transform/ultimate-insider-threat-north-korean-it-workers.

[2] Wells, R. 36% Of Job Adverts Are Fake—How To Spot Them In 2024. Forbes. 13 August 2024. https://www.forbes.com/sites/rachelwells/2024/08/13/36-of-job-adverts-are-fake-how-to-spot-them-in-2024/.

[3] Escalera,J. 2024 Recruiting Survey Finds 81% of Recruiters Have Posted Ghost Jobs: Ghost jobs continue to populate job boards. My Perfect Resume. 5 August 2024. https://www.myperfectresume.com/career-center/jobs/search/recruiting-trends#job-seekers-face-a-scary-number-of-ghost-jobs.

[4] Resume Builder. 3 in 10 Companies Currently Have Fake Job Postings Listed. 18 June 2024. https://www.resumebuilder.com/3-in-10-companies-currently-have-fake-job-posting-listed/.

[5] Gressin, S. You got the Job! Federal Trade Commision Consumer Advice. 24 April 2023. https://consumer.ftc.gov/consumer-alerts/2023/04/you-got-job.

[6] Vakulov, A. The Hidden Risks of Job Hunting: recruitment fraud and cybersecurity. Forbes. 3 March 2025. https://www.forbes.com/sites/alexvakulov/2025/03/03/the-hidden-risks-of-job-hunting-recruitment-fraud-and-cybersecurity/.

[7] Catacora, D. Rise in AI-Generated Resumes Overwhelms Recruiters with Low-Quality Applications. All Work. 13 August 2024. https://allwork.space/2024/08/rise-in-ai-generated-resumes-overwhelms-recruiters-with-low-quality-applications/.

[8] Todd, D. North Korean IT Workers Expand Global Reach and Tactics. Secure World. 3 April 2025. https://www.secureworld.io/industry-news/north-korean-it-workers-expand-reach.

[9] Perry, B. W.; Kinslow, T. A.; Zagger, Z. V. FBI Warns of Hidden Threats in Remote Hiring: Are North Korean Hackers Your Newest Employees? Ogletree Deakins. 20 March 2025. https://ogletree.com/insights-resources/blog-posts/fbi-warns-of-hidden-threats-in-remote-hiring-are-north-korean-hackers-your-newest-employees/.

[10] Lemos, R. DoJ Shakes Up North Korea's Widespread IT Freelance Scam Operation. Dark Reading. 21 May 2024. https://www.darkreading.com/vulnerabilities-threats/doj-targets-north-koreas-widespread-it-freelance-scam-operation.

[11] Justice.gov. Two North Korean nationals and three facilitators indicted for multi-year fraudulent remote information technology worker scheme that generated revenue for the Democratic People's Republic of Korea. 23 January 2025. https://www.justice.gov/usao-sdfl/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent.

[12] Cameron, H. Tennessee Man Used 'Laptop Farm' To Fund North Korean WMDs: DOJ. Newsweek. 9 August 2024. https://www.newsweek.com/tennessee-man-arrested-helping-north-korea-wmd-program-1936889.

[13] Matza, M. US woman accused of stealing identities to give North Koreans jobs. BBC. 17 May 2024. https://www.bbc.co.uk/news/world-us-canada-69024813.

[14] McMillan, R.; Volz, D. North Korea Infiltrates U.S. Remote Jobs—With the Help of Everyday Americans. The Wall Street Journal. 27 May 2025. https://www.wsj.com/business/north-korea-remote-jobs-e4daa727?st=SXc9jC.

[15] Justice.gov. Arizona Woman Pleads Guilty in Fraud Scheme That Illegally Generated $17 Million in Revenue for North Korea. 11 February 2025. https://www.justice.gov/usao-dc/pr/arizona-woman-pleads-guilty-fraud-scheme-illegally-generated-17-million-revenue-north.

[16] The Guardian. Don't accidentally hire a North Korean hacker, FBI warns. 17 May 2022. https://www.theguardian.com/world/2022/may/17/dont-accidentally-hire-a-north-korean-hacker-fbi-warns.

[17] Boyd, C. Rapid7 Q1 2025 Incident Response Findings. Rapid7. 4 June 2025. https://www.rapid7.com/blog/post/2025/06/04/rapid7-q1-2025-incident-response-findings/.

[18] Burgess, M. North Korean IT Workers Are Being Exposed on a Massive Scale. Wired. 14 May 2025. https://www.wired.com/story/north-korean-it-worker-scams-exposed/.

[19] Nandanwar, S. Beware of Fake Experience Letters: A Shortcut You Should Avoid at All Costs. LinkedIn. 17 October 2024. https://www.linkedin.com/pulse/beware-fake-experience-letters-shortcut-you-should-avoid-nandanwar-vk9af/.

[20] Indeed. Why Is There an Indeed Email on My Resume? https://support.indeed.com/hc/en-us/articles/360037819631-Why-Is-There-an-Indeed-Email-on-My-Resume.

[21] Reddit. Looking for a job today is a privacy nightmare. I am starting to believe the application process is being used as a new revenue stream, to obtain data from applicants for profit. https://www.reddit.com/r/privacy/comments/16ntr24/looking_for_a_job_today_is_a_privacy_nightmare_i/.

[22] Reddit. So sick of "assessments" when applying for jobs. https://www.reddit.com/r/UKJobs/comments/1hclann/so_sick_of_assessments_when_applying_for_jobs/.

[23] Reed. Your profile. https://www.reed.co.uk/help/profile.

[24] Paying to get paid: gamified job scams drive record losses. Federal Trade Commision. 12 December 2024. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/12/paying-get-paid-gamified-job-scams-drive-record-losses.

[25] FTC. Refund and Recovery Scams. https://consumer.ftc.gov/articles/refund-and-recovery-scams.

[26] Reddit. Task Scams. https://www.reddit.com/r/Scams/search/?q=task+scam.

[27] Jennings-Trace, E. North Korean hackers are targeting LinkedIn jobseekers with new malware - here's how to stay safe. Tech Radar. 7 February 2025. https://www.techradar.com/pro/security/north-korean-hackers-targeting-linkedin-jobseekers-with-new-malware.

[28] Moiz Haji Mustaq Lakadkutta, A. URGENT: I Nearly Executed a Malware-Laced "Coding Test". LinkedIn. 29 May 2025. https://www.linkedin.com/pulse/urgent-i-nearly-executed-malwarelaced-coding-test-lakadkutta-opije/.

[29] Reddit. "Recruiter" tried to hack me (full story on comments) – bitbucket link below. https://www.reddit.com/r/programming/comments/1i84akt/recruiter_tried_to_hack_me_full_story_on_comments/.

[30] Sherbakov. N. Security Alert. LinkedIn. https://www.linkedin.com/posts/nikita-sherbakov_security-alert-a-few-days-ago-a-colleague-activity-7303298099764977664-_xH-/.

[31] Skill Nuggets. Python eval() function. https://skillnuggets.co.uk/python-eval-function/.

[32] Palazzesi, A. Almost got hacked. LinkedIn. https://www.linkedin.com/posts/austinpalazzesi_cybersecurity-activity-7332878341227659265-qh2F/.

[33] Lakshmanan, R. North Korean Hackers Target Developers with Malicious npm Packages. The Hacker News. 30 August 2024. https://thehackernews.com/2024/08/north-korean-hackers-target-developers.html.

[34] Reddit. Is anyone else getting random messages from people that "claim" there A&R rep's from Sony music or inter-scop [SIC] records? https://www.reddit.com/r/soundcloud/comments/1jq08rh/is_anyone_else_getting_random_messages_from/.

[35] Reddit. Had a message from Sony. https://www.reddit.com/r/soundcloud/comments/1j5llun/had_a_message_from_sony/.