CSaaS SIG
An IT ISAC Community

DO YOU KNOW WHO YOU ARE HIRING?

Spotting Fraudulent Job Seekers

Product of the IT-ISAC Critical SaaS Special Interest Group (CSaaS SIG) with contributions from:

David Bradbury
David B. Cross
Jeffrey DiMuro
James Dolph
Ashlyn Jimenez
Kaitlyn Palatucci
Dhaval Parekh
Akshay Shetty

JULY 2025

INTRODUCTION

Hiring workers is an essential part of any organization's operations, and up until recently, it's been a fairly straightforward process. But what happens when the resources an organization onboards aren't who they say they are? A growing challenge, particularly in the technology space, is an influx of fake applicants who are scamming organizations into hiring them – often originating from adversary nations. Fraudulent actors present themselves as legitimate remote freelance candidates, falsifying credentials, stealing identities, generating resumes with AI, and even using deepfake technology to create various social media accounts, including LinkedIn profiles. As these technologies continue to advance, it becomes increasingly difficult to distinguish at first glance between authentic and fraudulent candidates. SpyCloud reports that around 10% of Fortune 500 companies have already interacted with, and potentially hired, fraudulent resources.

This phenomenon is not new – the Democratic People's Republic of Korea (DPRK) and other threat actors have long engaged in cyber-enabled financial crimes, but the sophistication and scale of these efforts have intensified significantly in recent years. In May 2022, the Department of State, the Department of the Treasury, and the FBI released a joint advisory regarding these scams; the advisory notes that some of the first reports on DPRK IT workers stem from a United Nations expert panel that reported on the topic in 2019. The FBI also released a January 2025 PSA on DPRK workers' data extortion, and more recently, the U.S. Department of Justice has announced coordinated efforts to deter the schemes in question, and has begun indicting and arresting associated individuals and searching "laptop farms" from which the fraudulent workers enact their scams.

While DPRK workers are the most recent and prolific in this space, these scams are a known issue. They have existed in many forms for a long time and will continue to persist, driven by a variety of sources and adversary nations. These workers' motivations are twofold: to generate revenue for their countries' regimes to fund various programs, as well as to infiltrate organizations for the purpose of stealing sensitive intellectual property, data, and technological know-how. These workers are often unqualified for the advertised role, but their true value lies in their ability to launder dollars and IP from US companies. Many of these scams are operated through third-party platforms and intermediaries, making detection and prevention even more challenging.

Despite red flags, the influx of remote workers in modern times has made companies vulnerable to this form of infiltration, and the scope of the threat continues to grow. By 2028, AI-generated job applicant profiles are projected to make up one in four candidates globally, posing a significant threat to hiring integrity.

With so many fake applicants on the market, and technology improving, how can organizations reliably identify and weed out job candidates that may be fraudulent? There are several tells and warning signs that hiring managers can watch for to indicate that an applicant may not be all they appear to be.

CANDIDATE APPLICATIONS

Applications often have plenty of indicators right out of the gate that an applicant may not be legitimate. Look for these signs as you review a candidate’s resume.

- **Applying to Different Roles:** An immediate tell is if an individual applies to not just one role, but multiple roles across several different departments – upon comparison, these applications may list subtly or vastly different levels and areas of experience. On the other hand, at times you may see identical or extremely similar applications submitted with different names; in either case, you’ve likely encountered a scam.

- **Inconsistencies and Vagueness:** Falsified resumes can be vague when it comes to listing out tangible experience, use generic language, lack the level of personalization of other candidates’ applications, and may notably have inconsistencies detailed such as erroneous locations or conflicting time zones. There can also be discrepancies in employment dates, job titles, and responsibilities. Sometimes they will have overlapping positions at multiple companies. Candidates should be able to describe their previous positions and roles very clearly and in detail.

- **Over-Polished Resumes:** Conversely, AI-generated resumes used by fraudulent workers may be overly refined or too “perfect”, and may additionally be stuffed with keywords to optimize for Applicant Tracking System (ATS) software.

- **Metadata Mysteries:** Check the metadata of your applicants’ resume files - there may be some telltale signs of tampering, such as registering a different author name than your applicant’s name.

- **No References**: All references should be validated and have accurate and complete contact information, as well as references that are reachable and interviewable.

- **Immediate Start Dates:** Candidates may insist on very fast start dates for remote work without clear reasoning, even though the position may be office-based or require a physical location. This is a red flag.

If these signals aren’t visible at a glance, there are plenty of additional precautions your team can take to target fraudulent applications.

Verifying Past Employers: It’s essential to check with each of a candidate’s listed past employers. Contact the companies directly using a direct line available on the organization’s website – do not rely solely on references provided by the applicant. Research the company’s online presence, physical address, and employee roster to evaluate its legitimacy. Consider using the “Organization Tree Crawl” method to map out real employees at the applicant's previous jobs - validating names, roles, titles, and other details. Often, fake employers will have no website or only a basic site with little verifiable information.

Cross-Validating Online Profiles: Investigating a candidate's online presence is also an essential step. Most candidates should have some form of footprint across social media – look for a LinkedIn profile and compare it with the application to confirm work history and double-check the individual's number of connections. A lack of activity on the internet or a sudden surge of recent work may be a sign of fraud.

Train Your Recruiters: If your organization works with recruiters, they are your first line of due diligence against fake applicants. Proper training is key – which includes ensuring that your team is familiar with the markers that may appear, flagging a fake resume or applicant. Use trusted platforms for collecting resumes, ideally ones that require verified identities and that maintain their own strong security protocols.

INVESTIGATING THE INTERVIEW PROCESS

Even if an applicant's resume gets the all-clear from your team, the interview process may reveal more indications of fraud along the way. Keep your eyes peeled for the below red flags and follow these best practices.

- **Ask for and Verify ID:** Before the interview begins, request a copy of the candidate's government-issued identification. It is recommended to always use an identity and/or background check service to validate identities before conducting interviews. This will often deter many fraudulent candidates from proceeding.

- **Mandate an In-Person Meeting:** Seeing is believing – if possible, at least one of your interviews with each candidate should take place in person. If an on-premise interview isn't possible, you might ask the candidate to come to the office after they've been hired – or even send an existing employee to meet with them if they live in the same area. Often setting the expectation of an in-person meeting will discourage fake IT workers from applying or continuing the interview process.

- **Keep All Interviews On-Camera:** It doesn't matter if a webcam is broken or a candidate is shy. All virtual interviews should take place on camera; and even if the interviewee seems to be legitimate via the screen, AI technology has made deepfake interviews all the more possible. Keep a critical eye out and watch for lag, camera blurs, or claims of technical issues – or tangible tells of interviewees taking calls from foreign countries, such as non-U.S. outlets or power boards in the background of the shot.

- **Don't Allow Virtual Backgrounds:** Virtual backgrounds can hide a number of things, including a candidate's actual location. In order to help verify they are where they say they are, ask candidates to turn off their backgrounds during interviews – and even encourage them to show the room they're in for added insurance that no other individuals are in the room and no aids are being used. Interviewers can also ask the candidate to show their hand in front of the camera, which will often reveal AI-generated content.

- **Use Threat Intelligence:** Organizations can strengthen their candidate screening and fraud detection processes by leveraging threat intelligence Indicators of Compromise (IoCs) to identify known bad IPs, fake personas, and stolen identities. By integrating real-time threat feeds and geolocating candidate IP addresses, companies can flag mismatches between a candidate's claimed LinkedIn location (for example) and their actual login origin. Correlating multiple indicators—such as suspicious IPs, reused identities, and location discrepancies—enables more accurate risk assessments and automated alerting, helping security and HR teams proactively detect and investigate fraudulent applicants.

- **Ask Off-Script Questions:** Going off-script can trip up candidates who may be using AI or another tool to generate interview answers. Try to ask an off-the-wall question that may not be expected during a job interview, such as "What is your favorite dessert?" and pay attention to the interviewee's response and how long it takes for them to answer.

- **Problem-Solving in Real Time:** Asking interviewees live problem-solving questions or encouraging them to use real-time collaboration tools can assist in determining whether they actually possess the skills they advertise on their resumes. Don't allow candidates to activate screensharing, as screenshares can be easily manipulated to look a certain way to hide tools like remote access or ChatGPT.

- **Panel Interviews Preferred**: Getting a second, third, or more opinions on each candidate is ideal. Interviewees should undergo at least one panel interview, and all interviewers should agree with one another before extending a job offer – if there is any concern, suspicion, or uncertainty, don't move forward with hiring.

- **Fraud Awareness Training for Recruiters and HR Teams:** Provide ongoing training sessions for HR and hiring/recruiter staff to keep them updated on new fraud types, techniques (e.g., sophisticated deepfake tools), and additional methods of spotting suspicious behavior.

- **Small List of Approved Vendors to Hire Contract Workers From:** Establish a list of approved staffing agencies and third-party vendors for hiring contractors or temporary workers. Conduct regular audits of these vendors to ensure their processes align with your organization's standards for verifying candidate authenticity. This reduces the risk of fraudulent candidates entering through less reputable or unverified sources.

AFTER ACCEPTANCE - NOW WHAT?

Perhaps all the boxes have been checked and you think your new remote worker is safe. We still recommend the following best practices even after the offer letter has been issued.

Double-Check the Address: Often, fraudulent workers will have laptops and other equipment sent to a non-residential address or a different location than the one listed on their resume as their home address. Double-check to ensure that the information adds up, and that you're not being asked to send technology to an unusual or distant location. You might even enforce a policy that the candidate must pick up the equipment in person, with any exceptions approved by the executive level when possible. Again, setting an expectation of in-person activities is an effective deterrent.

Look for Any Payroll Puzzles: Part of the onboarding process for a new role includes setting up payroll or payment methods. Ensure your new hire's bank information matches their name, and be aware of any frequent request changes to their bank. Don't provide non-traditional payment methods such as Venmo, Cash App, or crypto wallets.

Monitor Productivity and Work Performance: Employee productivity and work performance is always important, but in the context of fraudulent workers, be wary of those who refuse to work in collaborative platforms, miss deadlines without explanation, and favor text-based chat over videos or meetings. In a remote setting, it is also important to watch for inconsistencies in location, video background, appearance, etc.

Keep an Eye on KVM: Ensure that your new employee does not install any remote access tools on your organization's devices. IP-KVM devices, for example, allow for computers to be remotely controlled by Keyboard, Video, and Mouse through a network connection – without any software needed. Though not all of these types of devices are malicious, they can easily be used to support malicious behaviors, and should be monitored closely or disallowed.

Watch for Strange Behavior: Once the candidate has been logged into your organization's systems, keep your eyes peeled for any unusual behavior, such as attempting to gain access to data that is off-limits; large file downloads, uploads, or transfers; and requests for privileges that are unnecessary to complete their job. Flag any of these behaviors immediately.

Protect Yourself with These Precautions

- **Employee Training:** Employees can be a company's greatest vulnerability - an insider threat. Ongoing training for your staff can help individuals recognize suspicious behavior or irregularities, enabling them to take prompt action. Ensure that all training includes a clear and concise way for employees to report without fear of retaliation.

- **Principle of Least Privilege (PoLP):** Even after hiring, candidates should only be given access to the minimum systems and data necessary to perform their duties. By limiting their access from the start, you reduce the risk of data breaches or misuse of sensitive systems if the person turns out to be a bad actor.

- **Role-Based Controls:** These controls ensure that each user is only granted permissions based on their specific job role, making it easier to manage and audit access systematically.
- **Continual Monitoring and Auditing:** Organizations should keep an eye on activity at all times and watch especially for suspicious actions, attempts at access, unusual data downloads, and more.
- **Review Access Logs and IPs:** Sudden changes in IP address, especially from different countries, or access at unusual hours could indicate that work is being outsourced or that unauthorized users are logging in.
- **Consumer VPN or Remote Access Software:** Connections from consumer VPN services and/or use of consumer remote access software should be prevented on company devices where possible.
- **Stay Informed:** Communicating and sharing TTPs and other details with peer organizations through an ISAC can help your team stay informed of evolving strategies.

MY NEW HIRE MAY BE FRAUDULENT - HERE ARE YOUR NEXT MOVES

If you believe a candidate you've hired may be fraudulent, there are still ways you can manage impact and protect your organization's data. Use the following mitigations to prevent any further damage and quarantine the situation.

- **Suspend Access:** If you suspect an employee may be engaging in fraudulent activity, immediately isolate their access to all systems within your organization.
- **Report to Your Organization's HR and Legal Representation:** Any concerning behavior and confirmed IT scams should be reported to the company's HR and legal representation, whether internal or third-party, as these incidents may have a range of legal ramifications based on applicable laws and regulations.
- **Perform an Incident Review and Audit:** Be sure to thoroughly document the compromise via an incident review and audit the employee's level of access as well as the data that may have been compromised in the process.
- **Terminate Employment:** If credible evidence suggests a worker may be fraudulent and both HR and legal entities have been alerted, the worker should be isolated from payroll, internal communications, and all other employee portals as soon as possible. Be diligent in ensuring that all access has been fully revoked and no entry points remain.

CONCLUSION

The threat posed by fraudulent IT workers continues to evolve, riding the global shift toward remote work and exploiting the changing vetting processes that accompany this shift. These actors may appear as legitimate, highly qualified candidates, but with a scrutinizing eye, it is possible to identify the bad apples from the bunch and weed them out of the application process. To achieve this, organizations must enforce stricter hiring standards and continuously monitor to effectively identify and prevent such threats. A known impending in-person interaction, whether during the interview process or the onboarding phase, can help deter fake applicants from the onset.

A culture of healthy skepticism is essential when it comes to hiring remote workers. Trust should be earned over time and reinforced by evidence, not granted solely based on credentials or interview performance. From identity verification to post-hire audits, a cautious and methodical approach means the difference between hiring a valuable team member and unwittingly aiding a hostile foreign operation. In today's world, protecting your organization requires not just a strong cybersecurity posture but vigilance at every stage of the hiring lifecycle.

IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

INFORMATION TECHNOLOGY - INFORMATION SHARING AND ANALYSIS CENTER (IT-ISAC)

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

CSaaS SIG

An IT ISAC Community

CRITICAL SaaS SPECIAL INTEREST GROUP (CSaaS SIG)

The Critical SaaS Special Interest Group (CSaaS SIG) is part of the IT-ISAC and serves as a forum for CSaaS companies to collaborate on a collective defense strategy to improve the security and operational resiliency of their services and share intelligence information with the industry. It enables companies who are essential to the internet to share cyber threat intelligence and effective security practices. The SIG holds a weekly analysts meeting and is designed for security managers, analysts, and IT executives from Critical SaaS companies.