Red Flags to Look for in Video Interviews with Remote IT Workers

Hiring remote IT workers, especially for sensitive roles, comes with its own set of challenges. With the growing concerns over security breaches, espionage, and data integrity, it's crucial to identify potential warning signs during the interview process. Here are some red flags to look out for when conducting video interviews with remote IT workers, especially considering rising global threats and concerns, such as those highlighted by the case of a US security firm unknowingly hiring a hacker from North Korea.

1. Uncooperative or Evasive Behavior

- **Reluctance to Answer Key Questions**: If a candidate hesitates or evades direct questions, especially when asked about their experience, work history, or connections to foreign entities, this could signal dishonesty or hidden affiliations. Evasive responses on sensitive topics like past employers or security clearances might indicate something is amiss.
- **Avoidance of Eye Contact**: While eye contact can be harder to maintain on video calls compared to in-person interviews, consistent avoidance could be a sign of dishonesty, nervousness, or lack of transparency. A candidate who struggles to engage visually may be hiding something.

2. Technical Difficulties

- **Frequent Connection Issues**: Although occasional technical issues are common, repeated disruptions during the interview could be a red flag. Persistent connectivity problems might indicate that the candidate is not working from the location they claim, or worse, they could be using tools to mask their actual location.
- **Suspicious Delays or Glitches**: Sometimes, artificial technical difficulties are used to cover for location masking tools, such as VPNs or remote desktop protocols that might be employed to hide a candidate's true location.

3. Unusual Background

- **Suspicious or Unfamiliar Surroundings**: Video backgrounds can reveal a lot. If the candidate's surroundings seem inconsistent with their claimed location (e.g., they claim to be in one country, but their environment suggests another), this could be an indicator of deception. Additionally, the use of virtual backgrounds might be a way to obscure their real surroundings, raising suspicions.
- **Inconsistent Work Setup**: IT professionals, especially remote ones, usually have a well-organized technical setup. A disorganized or unprofessional setup could indicate that the candidate is not fully prepared or truthful about their working environment.

4. Inconsistent Information

- **Contradictions in Responses**: Inconsistencies in a candidate's responses, particularly related to their work history, qualifications, or technical experience, should be carefully scrutinized. These contradictions may be attempts to misrepresent themselves or fabricate credentials.
- **Gaps in Resume or Unexplained Employment History**: If a candidate is unable or unwilling to provide a clear timeline of their employment or projects, this could indicate involvement in activities they want to conceal.

5. Overly Confident or Arrogant Behavior

- **Excessive Boasting**: Candidates who exhibit overconfidence or boast excessively about their skills or accomplishments may be compensating for gaps in their knowledge or experience. This could also be a tactic to distract from security vulnerabilities in their background.
- **Dismissive of Questions or Criticism**: Candidates who respond dismissively to questions or feedback, especially regarding security protocols, might lack a critical understanding of the industry's demands or have something to hide.

6. Limited Knowledge of the Company or Industry

- **Lack of Familiarity with the Company**: If a candidate seems unprepared to discuss your company, its products, or its industry, this is a red flag. This lack of preparation might suggest the candidate is not genuinely interested in the role and could be applying for other reasons, such as gathering information for malicious purposes.
- **Unclear Understanding of IT Security Principles**: A remote IT worker must be highly knowledgeable about security protocols, especially if the role involves handling sensitive data. If the candidate shows limited knowledge of these critical issues, it could indicate they are not fit for the position or worse, have malicious intent.

7. Suspicious Online Activity

- **Red Flags in Background Checks**: A thorough background check, including social media profiles and online activity, can reveal warning signs. Connections to foreign entities, involvement in suspicious online forums (especially those related to hacking or espionage), or other questionable online behavior should not be ignored.
- **Untraceable or Sparse Online Presence**: While some professionals may not maintain an extensive online presence, the complete absence of any digital footprint in today's connected world could be a cause for concern. It could mean that the individual is deliberately hiding their identity or past affiliations.

8. Unusual or Unexplained References

- **Refusal to Provide Specific References**: If a candidate is unwilling to provide references or only offers vague contacts who can't be reached or verified, this could indicate a lack of legitimate professional connections.
- **Foreign-Based References without Clear Explanation**: Particularly for high-security roles, it's essential to verify the credibility of any international references, especially if the candidate has links to countries with known security concerns.

Did you find this research paper of value? Here are some of our other research papers.

1. IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company

2.Secrets of Hiring and Firing vCISOs

3.CMMC Compliance-The New Enclave Approach

4.The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis

5.When Management Fails: How the IT Folks Can Protect Their Jobs After a Breach

6.Monitoring Your IT Systems-The Best Tools That Meet Compliance Requirements and Which are Affordable for SMEs