



## IS YOUR NEW HIRE WHO YOU THINK?

BY JAY BORDEN

North Korea has a new trick, they get you to hire one of their people. Sound impossible? But it is happening. Way more often than many companies admit.

Implausible as it seems it is working. A cybersecurity firm found 40% of its clients had North Koreans working for them. The US Department of Justice found 300 companies had these workers. The problem is pervasive.

The process to get these workers into companies is complex. Let's take a look.

Candidates apply for remote work positions through the company's website or through popular job boards. Devious tricks are used to conceal their real identity. Someone else may do the interview for them. Someone of Asian ancestry to match the surname but fluent in English. Sometimes the applicant knows limited English, enough to get through the interview.

Another trick is to use Asian American college students who are willing to let these applicants use their identities in return for money.

The candidate can't be in North Korea due to international sanctions. The candidates are typically located in countries friendly to North Korea such as Russia or Malaysia and where the internet and electric grid are more reliable.

The candidates are kept as virtual slaves housed and fed in communal settings and all their actions monitored and controlled. Their families in North Korea are used as leverage to keep the people working. The majority of their earnings are shipped back to North Korea, not to the family but to the government.

Now they need a company laptop. Shipping laptops to Russia or Malaysia would be suspicious. Instead, the laptop is shipped to a legitimate address in a friendly country, possibly even in the USA.

**IS YOUR NEW HIRE WHO YOU THINK?**

CONTINUED

But that location isn't where the new hire is, it is a laptop farm that houses laptops for a number of these North Koreans. Each North Korean worker is then given remote access to the correct laptop by the manager of the laptop farm.

Once they have the laptop and begin working they may also begin to look for data of interest to the North Koreans or to insert malware in the applications or devices.

So how to find these imposters?

The deception is devious and complex making it difficult to detect. How many North Koreans are actually employed by American companies isn't known but is estimated to be significant.

Any job applicant will need to be interviewed. Be sure it is on a video call and ask them to show picture identification. If they present any reason why they cannot be on a video call it is a red flag. Even if they are on the video call and show a picture ID know they often use stolen or synthetic identities. So, a video call may not be enough to identify fraudulent applicants.

During the interview see if they wait before answering a question or repeat the question first. This gives them or an accomplice time to search the internet for an answer.

Ask where they grew up. See if the answer matches the resume. Does their accent match the country where they say they were born or raised? If possible have someone who speaks the native language of that country in the interview to speak to them in that language. If they don't understand, another red flag.

Ask about their favorite spot in that town. They may not know one. What is their favorite restaurant? Again, harder to answer if you haven't been to the town. May find this by internet search so ask about their favorite dish. Then ask more about it. Set a trap. Say the dish is different than the same dish in other restaurants. Do they like the unique flavor in that restaurant or the more conventional flavor of the dish in another restaurant? Maybe ask about the decor of the restaurant. Or anything that will show if they have ever been there.

**IS YOUR NEW HIRE WHO YOU THINK?**

Continued

Ask about favorite local events, sports teams and favorite players. Put in errors such as saying the wrong team won a recent game. Say you really liked a play they made but you just made up. See if they know what really happened. A real fan would know.

Ask about hobbies. Do they sound plausible for the location? In one example we heard about a candidate said their favorite sport is badminton. That is popular in some Asian countries but not in America.

Is your IT monitoring of their laptop finding anomalies. Are they working strange hours like overnight? Do they check email only on the laptop and not on a mobile phone? Most legitimate workers would check email on both devices. But the phone would not go through the laptop farm in the neutral location and would give away their real location.

Does the laptop have kvm, keyboard, video monitor, mouse software installed? This wouldn't be needed for someone working directly on the device but is necessary for remoting in.

Have they attempted to circumvent the protections on the laptop and install unauthorized software? Did they use a VPN other than the official one?

While no one answer may be sufficient to identify a North Korean applicant, taken together they may show a pattern of behavior that is indicative of something else going on.

If something is detected we suggest alerting the FBI and other authorities. They may work to locate the laptop farm and close it down.

Stay alert and good luck.

Visit our site, [onebrightlycyber.com](http://onebrightlycyber.com) to learn all the ways we help keep you safer.

Welcome to peace of mind.