INSIGHTS
Cyber made simple.

one brightly cyber

SOCIAL ENGINEERING IS THE BIGGEST RISK

BY JAY BORDEN

We recently wrote about AI being used to both write job postings and the resume/cover letters to apply to them. We joked that the next step may be that AI posts the position, AI applies for the position and AI gets the position. As sometimes happens, what is said in jest becomes real.

Today, many people work remotely or in the field and are being interviewed over video systems like Zoom or one of the others. But deep fakes are being used on these video interviews. The quality of the deep fakes is so good it can be difficult to determine if the person is real or not.

This presents a challenge to HR departments. Further complicating the hiring process is that deep fakes are being used to mask candidates who aren't permitted to work in this country. There have been a number of them found to be North Koreans. The person is real, it's just who appears on the video interview is not real, a deep fake or maybe someone hired to do the interview.

The real people do the work and get paid. But the money winds up in North Korea with the government as a way to circumvent the economic sanctions.

This technique is so effective KnowBe4, a well know cyber education company hired one of them. KnowBe4 has extensive protections in their hiring process, but this person made it past all the safeguards and was hired. They were caught when they attempted to download and install software on the company provided laptop. The security protections against installing software prevented it and resulted in the scheme being discovered.

I'm not betraying anything confidential, KnowBe4 made this public as a service to everyone. Many large companies admitted they probably had North Koreans working for them also who had not been caught.

SOCIAL ENGINEERING IS THE BIGGEST RISK

CONTINUED

Besides the money aspect, employees have access to internal information, systems and more. All desired by North Korea. Be sure to examine your hiring process from start to finish for gaps or lapses that may allow these people through.

In another instance, a deep fake of a company executive was used to convince a finance employee to wire money immediately to a new account. The employee did it and the company was out $25 million. Cybercriminals don't offer refunds.

Not content with using AI and deep fakes in the hiring process, cybercriminals are now exploiting the employment termination process.

They are sending termination notices to employees with attachments to click for more details. Very understandable that receiving this type of a notice makes you nervous. Of course, you click the link and provide confidential information to "login" to the system. Once you enter your information it is in the hands of the cybercriminals.

The email notices look very real. In a recent case in the UK, the notice came from the UK Employment Tribunal and had all the right seals, logos and case numbers. As is typical with scams you are told to take immediate action, in this case to avoid legal consequences. Cybercriminals don't want you to take time to think about it. No wonder people are taken in.

One more example. A short summary of a scam that went on for months. A woman received a phone call with caller ID saying it was her local police department. The officer said her Social Security number had been used in crimes. Since it was federal, they would transfer her to the FBI agent in charge. The "FBI agent" explained the seriousness of it and asked if she would help catch the criminals doing this. Of course, she agreed. Over the next months she spoke to the FBI agent every day, sometimes more than once a day. The end result of it? Her bank account and savings were drained.

What do all these examples have in common? They all depend upon people being fooled by social engineering.

Research has shown that people are the cause of 70% of breaches. Some research puts that figure closer to 90%.

HE HIRING PROCESS,

SOCIAL ENGINEERING IS THE BIGGEST RISK

CONTINUED

If we believe that research which has reached the same conclusion for years, possibly even decades, then why isn't more emphasis put on educating and training people to spot social engineering? Granted, some of the schemes are elaborate as the above examples show. But training to identify social engineering red flags and regular desktop exercises to see who still is caught by it should help reduce the risk.

If criminals are breaking into houses through the windows, will you put more locks on your front door while ignoring the windows? Hopefully not. The same thing is true here. How much is spent on tools and other protections while ignoring the serious threat of social engineering?

We aren't saying to stop buying tools. We're just saying look at where the biggest risks are and act accordingly.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.