If a Cybersecurity Firm Can Fall For the Latest AI Workplace Scam, So Can You: 10 Steps to Protect Your Business

Insights
8.01.24

A prominent cybersecurity training company just fell victim to an increasingly common scam when it hired a remote worker who turned out to be a North Korean cybercriminal that used AI deepfake tools to fake his identity and infiltrate the organization. The Florida-based company caught the would-be thief before he was able to steal any data, but he did attempt to load malware and execute unauthorized programs on firmwide systems in what could have been a damaging attack. "If something like this can happen to us, it can happen to almost anyone," the CEO said in the wake of the cyberattack. What are the 10 things you can do to ensure you don't fall for the same scam?

What Happened?

- The Florida-based firm, which specializes in providing cybersecurity training across the globe, was hiring a remote software engineer for its internal IT AI team.
- It ended up hiring a remote worker for the job after a typical hiring process. It selected resumes from the applicant pool, conducted four video conference interviews for the leading candidate, confirmed by video that he matched the photo provided on his application, ran a standard background check, and even verified references before hiring him.
- The company sent the new hire a computer workstation on July 15, and he immediately attempted to load malware the moment he received it.
- Alarm bells went off in the company's IT security department, and they reached out to the new hire to ask what was going on. At first, the new hire explained he was simply troubleshooting a tech issue. When IT tried to get him on a phone call to inquire further, he said he was unavailable and then became unresponsive. Within 30 minutes of him activating his computer, the IT team shut down his access, and the company then terminated his employment.

What *Really* Happened?

The following information comes straight from the company CEO himself, who explained in full what happened in a series of blog posts.

- The cybercriminal was using a valid but stolen identity of a U.S. citizen. He used AI tools to enhance a stock photo and make it appear like a brand-new person. You can see a side-by-side

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

comparison of the stock photo and the applicant's faked photo here.

- He most likely used AI tools to alter his voice, and may have also used AI technology to change his image (as was successfully done in the recent $25M Hong Kong heist).
- The fake worker had his company computer sent to a physical address somewhere in the U.S. that turned out to be an "IT mule laptop farm." He then used VPN to mask where he actually was – which turned out to be in North Korea or right over the border in China.
- He worked in the middle of the night in Asia to make it seem like he was working in the daytime here in the States.
- Other details about the attack are not yet available because the matter is part of an active FBI investigation, but the point remains – if it can happen to a cybersecurity company, it can happen to you.

What Do These Scams Hope to Accomplish?

There are a few reasons why someone might try to fake their identity to join your company.

- In some instances, the fake worker could be part of a network of state-funded North Korean cybercriminals who are flooding the remote work environment in attempts to get hired by U.S.-based companies. In these instances, they will actually do real work for an organization. A large amount of the money they are paid for their work will end up funding North Korean state actions.
- In the instance described above, it appears the cybercriminal had a more malicious intent. In the very short time he had access to company equipment, he manipulated session history files, transferred potentially harmful files using a raspberry pi, and executed unauthorized software. While his end goal remains unclear, he could have been attempting to cause disruption to company services and may have wanted to extract a ransom in a blackmail-type exchange. Or he may have been hoping to extract information left on the computer before the company commissioned it to him.
- The fake employee didn't have access to any company systems or information, but other AI scammers use these types of infiltration opportunities to steal company data. You might find your organization at a competitive disadvantage if your company information is leaked to the public, or you could find that information for sale on the black market.

10 Steps to Protect Your Organization in the Remote Work Era

- Foster a **culture of skepticism** when it comes to hiring remote workers, similar to the way that employees are now on guard for phishing emails.
- Train your hiring team on **social engineering tactics** now being employed by malicious cyberattackers.
- Conduct all video interviews with the camera on and train your hiring team to look for **deepfake signatures** (blurry details, irregular lighting, unnatural eye or facial movements, mismatched

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

audio, absence of emotion, etc.). As technology improves, you should also consider investing in threat-detection tools that can identify and flag potential deepfakes.

- Consider the feasibility of conducting **in-person interviews**, even for remote positions. Even mentioning that the process includes an in-person interview may dissuade scammers from continuing with the interview process.
- Make sure any laptops provided to new hires are **completely wiped clean** of any residual company data, including data stored on web browsers.
- Only ship laptops to **physical addresses** where the employee lives. Or send them to a trusted third-party (like a reputable delivery service office) where new employees are required to provide a valid picture ID to obtain them.
- Start new employees in a **highly restricted environment** where they only have access to the systems necessary to perform their work. Ensure they don't have immediate access to production systems or sensitive data.
- Ensure your **IT security monitoring systems** are robust and up-to-date, trained to look for attempts to access unauthorized systems or download improper files.
- **Audit all of your hiring practices** to ensure your hiring team is consistently following best practices on background checks, references, resume review, interviews, and more.
- Conduct regular **security training awareness sessions** for all employees on the latest cybersecurity threats and how to recognize and report them.

Conclusion

We will continue to provide the most up-to-date information on workplace data security and AI-related developments, so make sure you are subscribed to Fisher Phillips' Insight System. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Group or AI, Data, and Analytics Practice Group.

Related People

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

Richard R. Meneghello
Chief Content Officer
503.205.8044
Email

David J. Walton, CIPP/US
Partner
610.230.6105
Email

Service Focus

AI, Data, and Analytics

Counseling and Advice

Privacy and Cyber

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.