scaut

The risks

Can you risk hiring people you know nothing about?

There are many reasons for you to ensure compliance and security in your hiring process. Are you doing enough to mitigate the risks your business is facing?

Are you protected from these risks?

Non-compliance
With EU and national regulatory requirements to secure critical infrastructure (NIS 2, CER and more), obligations to have a secure workforce are increasing.

Supply chain vulnerability
With the ever increasing ability to work remotely, contractors with hostile intent can easily assume false identities and join your team. The supply chain is often used as a vector of attack in cyber-crime.

Identity theft
Fraudulent employees can misuse colleagues' or clients' personal information for their own enrichment or other illegal activities.

Data theft
Unauthorized access to company data can lead to its theft, which puts client privacy and company trade secrets at risk.

Financial fraud
From payment diversion to asset misappropriation, financial fraud can cause huge financial losses for companies.

Reputational damage
Hiring the wrong person can cause significant loss to financial capital, social capital and/or market share.

Recruitment fraud accounts for 24 Billion GBP lost in the UK alone

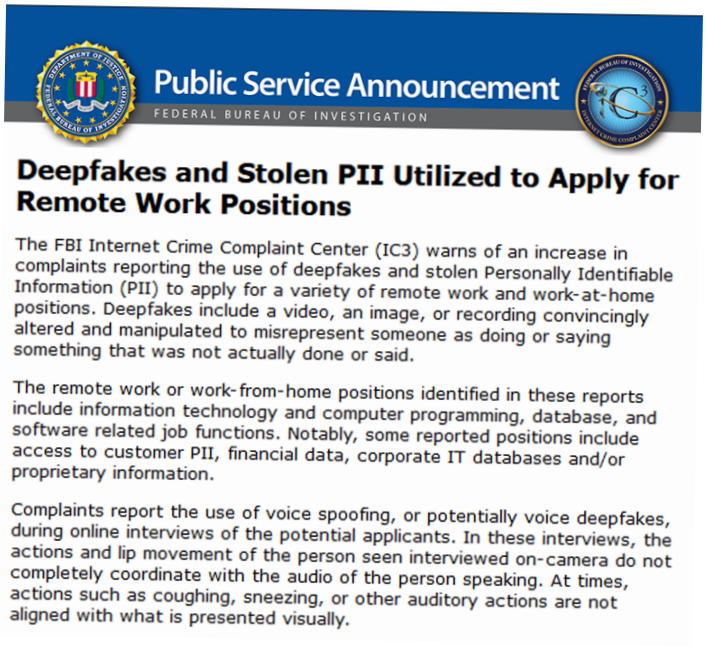
The Association of Certified Fraud Examiners estimates **organizations lose an estimated 5% of their annual revenue to fraud**, with a significant portion attributed to **actions taken by insiders.**

Organizations investing in people controls like screening have been shown to experience smaller losses and detect fraud more quickly. **Talk to Scaut today.**

Alert: Fake Software Engineers from China Infiltrating European Businesses

Companies in Europe have recently encountered a remarkable phenomenon: IT candidates who, according to the documents they provided to their prospective employer, should be sitting at a computer somewhere in Europe are actually in China.

This was the case of one of the Czech technology startups that MF DNES met (due to the sensitivity of the case, the editors did not mention the name of the company). A person interested in the job of a full-stack lead developer applied for the job via the social network LinkedIn. According to the documents he provided to the company, he was a Danish citizen living in Denmark. He successfully passed several rounds of the recruitment process, which also tested his programming skills. However, the information he provided to his prospective employer did pass the rigorous screening process at Scaut.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

"When we followed the trail of the linkedin profile, we found that it was connected with other suspicious profiles. They all have common characteristics, they try to give the impression that these people are graduates of European universities and usually work remotely for a long time, for example from Serbia or Estonia," says Petr Moroz, CEO of Scaut, which screened job candidates for the company.

The network of hundreds of LinkedIn profiles then converges on the Chinese city of Dandong, a city of two million near the border between China and North Korea. The city is home to, among other things, a Chinese army base.

That the Chinese intelligence services may be behind the activities of the 'fake A.I.' is just one theory. However, the largest domestic secret service, the BIS counterintelligence agency, has long warned against Chinese activities on Czech territory, and so has the FBI in its public warnings from...

Learn more about protecting your company. Talk to Scaut today.

source: excerpt from scaut.com/en/blog